

Università della Svizzera Italiana  
Facoltà di Scienze della Comunicazione  
Lugano

---

**Analisi degli aspetti tecnici e  
comunicativi dello spamming sulla base  
di informazione documentaria e di test  
effettuati in rete**

memoria di licenza

di

*Marco Faré*

Matr. Nr. 94-912-318

relatore: prof. *Fiorenzo Scaroni*

Anno Accademico 2002/2003

## Indice generale

<b>1. Introduzione</b>	<b>1</b>
1.1. La posta elettronica	1
1.2. Lo spamming	1
1.3. Struttura della memoria	3
1.4. Ringraziamenti	4
<b>2. Definizione</b>	<b>5</b>
2.1. Alcune definizioni	6
2.2. La definizione scelta	10
2.3. Contenuti	12
2.3.1. Categorie	12
2.3.2. Truffe e fenomeni simili allo spamming	14
2.4. Lo spamming fuori dalla Rete	16
2.5. Lo spamming è uno scomodo parente dell'e-mail marketing?	17
2.5.1. Definizione e particolarità dell'e-mail marketing	18
2.5.2. Un indirizzario onesto: compilazione e manutenzione	19
2.6. Origine del termine spam	20
<b>3. Basi tecniche</b>	<b>23</b>
3.1. Il sistema di posta elettronica su Internet	23
3.2. Il problema del relay aperto	24
3.3. Struttura del messaggio	26
3.4. Panoramica su SMTP	27
3.5. Esempio di analisi di un messaggio di spam	29
3.5.1. Header completo	29
3.5.2. Analisi	30
3.5.3. Conclusioni sull'analisi	31
<b>4. Storia ed etica</b>	<b>33</b>
4.1. Da Usenet all'e-mail e oltre	33
4.1.1. Alla fine degli anni Settanta	33
4.1.2. Dagli anni Ottanta agli anni Novanta	35

4.1.3.	Anno 1994: il fenomeno di massa	35
4.1.4.	Lo spamming arriva via e-mail	37
4.1.5.	La Usenet Death Penalty	38
4.2.	Lo spam è davvero un problema?	39
4.3.	Questioni di etica	44
4.3.1.	La Netiquette	44
4.3.2.	Oltre le Netiquette	46
4.3.3.	Etica nella lotta	47
4.3.4.	Le opinioni degli spammer	48
<b>5.</b>	<b>Le vie degli spammer</b>	<b>50</b>
5.1.	La spedizione	50
5.1.1.	Tramite ISP	50
5.1.2.	Relay aperto	50
5.1.3.	Relay multihop	51
5.1.4.	No relay	51
5.1.5.	Sistemi misti	51
5.1.6.	Il software	51
5.2.	Gli indirizzari	53
5.2.1.	Da Usenet	53
5.2.2.	Da altre fonti	54
5.2.3.	Generazione automatica	55
5.3.	All'interno del messaggio, tecnicamente	57
5.4.	Si guadagna?	58
5.4.1.	La regina dello spam	58
5.4.2.	Il (nuovo) re dello spam	60
<b>6.</b>	<b>Spamming e legge</b>	<b>61</b>
6.1.	Legge sì o legge no?	62
6.2.	Opt-in e opt-out	63
6.2.1.	Definizioni	63
6.2.2.	Implicazioni	63
6.2.3.	Il "listone" opt-out	64
6.3.	La tutela della privacy: TRUSTe	65
6.4.	Leggi sullo spamming nel mondo	66
6.4.1.	In Italia	67
6.4.2.	Nell'Unione Europea	68
6.4.3.	In Svizzera	68
6.4.4.	Negli USA e in Giappone	69
<b>7.</b>	<b>Contromisure tecniche</b>	<b>70</b>

7.1.	Organizzazioni	71
7.2.	Strumenti per l'utente	73
7.2.1.	Tecniche per i forum	73
7.2.2.	Tecniche per le pagine web	75
7.2.3.	Filtri e software: alcuni esempi	76
7.2.4.	Reverse Spam Filtering	79
7.2.5.	Filtri bayesiani	79
7.2.6.	L'utente reagisce: il reporting individuale e SpamCop	81
7.3.	Strumenti per l'amministratore di server e-mail	82
7.3.1.	Filtri in uscita e in entrata	83
7.3.2.	Le RBL	85
7.3.3.	MAPS: Mail Abuse Prevention System	87
7.3.4.	Spamhaus	88
7.3.5.	SPEWS: Spam Prevention Early Warnign System	89
7.3.6.	ORDB: Open Relay DataBase	89
7.3.7.	Altri prodotti commerciali	90
7.3.8.	I filtri web: Hotmail	90
7.4.	Soluzioni a lungo termine	91
7.4.1.	Server che strozzano	91
7.4.2.	Francobolli elettronici	94
7.4.3.	Tag per invii di massa	96
7.4.4.	Riconoscere la massa	98
<b>8.</b>	<b>Test in rete</b>	<b>101</b>
8.1.	Newsletter	101
8.1.1.	Scopo del test e iscrizione alle newsletter	101
8.1.2.	Risultati e commento	102
8.2.	Usenet e web	104
8.2.1.	Scopo del test	104
8.2.2.	Pubblicazione degli indirizzi	104
8.2.3.	Preparazione dell'analisi	105
8.2.4.	Risultati	107
8.2.5.	Grafici dell'andamento	108
8.2.6.	Commento	111
8.2.7.	Confronto tra i gruppi di discussione	111
8.3.	Altri test	112
8.3.1.	Confronto tra indirizzi	112
8.3.2.	Filtro anti-spam per webmail	114
8.3.3.	"Toglimi" nell'indirizzo mittente	114
8.3.4.	Indirizzario da Usenet	114
8.4.	Commenti finali	115
<b>9.</b>	<b>Conclusione</b>	<b>116</b>

---

<b>10. Indici delle tabelle e delle figure</b>	<b>120</b>
10.1. Indice delle tabelle	120
10.2. Indice delle figure	120
<b>11. Bibliografia</b>	<b>121</b>
11.1. Siti web	121
11.2. Libri	122
11.3. Leggi, decreti e direttive	122
11.4. Articoli	123
<b>12. Allegati</b>	<b>129</b>
12.1. Citazioni originali	129
12.2. Netiquette: etica e norme di buon uso dei servizi di rete	132
12.3. Gennaio 2003: Spam Conference	134

# 1. Introduzione

## 1.1. La posta elettronica

La posta elettronica nasce all'inizio degli anni Settanta e diventa rapidamente un mezzo di comunicazione importante: nel corso degli anni Ottanta le istituzioni accademiche scambiano regolarmente messaggi e-mail mentre Internet, la Rete delle reti, si espande e consolida la sua struttura. Dopo l'esplosione del World Wide Web, a metà degli anni Novanta, la posta elettronica assume un'importanza sempre maggiore anche al di fuori dell'ambito accademico. Oggi essa è utilizzata da istituzioni, aziende e privati per comunicare e scambiarsi dati. Secondo uno studio<sup>1</sup>, sono 600 miliardi i messaggi in circolazione nel 2002 per la sola Europa, con un incremento del 18% rispetto all'anno precedente. È un'applicazione tanto utilizzata che qualcuno la definisce la killer application di Internet. Sebbene si possa discutere su quest'ultima affermazione, è certamente vero che la posta elettronica è uno dei mezzi di Internet più utilizzati, rivelandosi ottimale per la comunicazione a distanza scritta e asincrona.. Altri tipi di applicazione (chat o forum su web, per esempio) stanno prendendo piede, ma oggi l'e-mail è uno strumento di lavoro per molte persone che spesso sostituisce la posta cartacea.

## 1.2. Lo spamming

Un fenomeno indesiderato legato alla posta elettronica è quello dello spamming, inteso quale invio di messaggi di posta elettronica a un gran numero di destinatari senza che questi li abbiano richiesti. Questa prima definizione introduce l'oggetto di questa memoria di licenza, che ha lo scopo di descrivere questo fenomeno da un punto di vista tecnico e comunicativo. L'analisi, di tipo documentario, è accompagnata da un test effettuato in rete grazie alla collaborazione dei servizi informatici e telematici TI-EDU<sup>2</sup>.

Lo spamming è un problema: l'intasamento dei server e delle caselle degli utenti mette in pericolo tutto il sistema di posta elettronica su Internet, sia dal punto di vista tecnico che da quello comunicativo. E per di più è in continua crescita: secondo alcuni osservatori un

---

<sup>1</sup> **Redazione Punto Informatico**, *200 mln di email al giorno in Italia*, 20 dicembre 2002, in Punto Informatico, <http://punto-informatico.it/p.asp?i=42580> (consultato il 20 dicembre 2002).

<sup>2</sup> **TI-EDU** (<http://www.ti-edu.ch/>) è la rete per l'insegnamento superiore e di ricerca scientifica nella Svizzera italiana (Cantone Ticino).

messaggio e-mail ogni sei è spam<sup>3</sup> e, dal 2007, ogni americano potrebbe ricevere 3.600 messaggi di spam all'anno. È comunque difficile trovare delle statistiche attendibili, data la natura decentralizzata di Internet. Tuttavia, confrontando numerose fonti si ottiene la conferma di questa tendenza. Sono in molti a prevedere che nel corso dei prossimi anni lo spam sarà uno dei problemi più visibili dello sviluppo di Internet. È però uno dei molti problemi di Internet, e probabilmente nemmeno uno dei più gravi: i problemi etici relativi alla privacy e alla sicurezza sono meno spettacolari ma richiedono riflessioni politiche di maggior spessore.

Non possiamo permetterci di sottovalutare questo problema e di considerare questi messaggi solo un fastidio: lo spamming genera un effettivo danno economico a tutti gli attori coinvolti professionalmente e privatamente nell'uso di Internet. Utenti e provider rischiano di subire una vera inondazione che compromette i sistemi tecnici e impedisce un flusso di comunicazioni confortevole. È quindi più di un fastidio trascurabile. La pericolosità del fenomeno deriva dal numero dei soggetti che inviano spam, che può essere molto elevato a causa dei bassi investimenti necessari all'invio. Il fenomeno si differenzia da quelli che analogamente accadono nel mondo reale, il mondo fuori da Internet, fatto di carta e di telefoni. Nel mondo reale, il mittente deve sopportare dei costi non indifferenti mentre su Internet la maggior parte delle spese ricadono sui destinatari e sugli intermediari, senza che questi abbiano la possibilità di opporsi.

In questa analisi, ho preso in considerazione soltanto lo spamming via e-mail, occupandomi secondariamente di quello sui gruppi di discussione Usenet che, pur presentando alcune analogie tecniche, resta comunque un fenomeno differente. Altri fenomeni, che talvolta vengono definiti spamming per via di una certa somiglianza, ma che mantengono una differenza sostanziale soprattutto sul lato tecnico, non verranno trattati. Mi riferisco in particolare allo spamming che arriva tramite programmi di chat dedicati o tramite telefono cellulare.

Durante la stesura della memoria ho cercato di descrivere il fenomeno e di proporre i mezzi per combatterlo, mantenendo il punto di vista dell'utente finale e quello degli intermediari. Inizialmente mi sono concentrato sulle contromisure, tecniche e legali, ma presto ho compreso che non sarebbe stato possibile affrontare il fenomeno senza definirlo adeguatamente. E questo si è rivelato un compito più importante del previsto: se è abbastanza semplice riconoscere un messaggio di spam, non è così scontato darne una definizione formale abbastanza precisa da circoscrivere il fenomeno senza essere troppo restrittiva. I siti delle organizzazioni anti-spam forniscono definizioni diverse, a volte in contraddizione tra loro. È necessario arrivare a una definizione unica, accettata da tutti, se si vuole combattere con successo lo spamming

---

<sup>3</sup> **Redazione Punto Informatico**, *Sorpresa..? Un'email su sei è spam*, 18 ottobre 2002, in Punto Informatico, <http://punto-informatico.it/p.asp?i=41819> (consultato il 20 dicembre 2002).

garantendo l'uso della posta elettronica per quegli scopi per cui è stata creata e per cui va considerata un mezzo di comunicazione prezioso e legittimo. Per questa ragione, è necessaria una definizione che distingua lo spamming dall'e-mail marketing in modo che la posta elettronica possa essere utilizzata quale veicolo promozionale in modo legittimo e accettato da utenti e aziende desiderose di investire in questo campo. Lo spamming deve anche essere distinto dai messaggi in broadcast su gruppi chiusi, come possono essere quelli delle aziende nei confronti dei loro dipendenti o delle scuole nei confronti degli studenti. Non bisogna nemmeno dimenticare di salvaguardare la comunicazione tra individui, anche anonima. Se, un giorno, qualcuno rinuncerà a spedire un e-mail di auguri natalizi agli amici per la paura di essere perseguito legalmente come spammer, allora la lotta allo spamming sarà stata un fallimento perché avrà creato quegli impedimenti alla comunicazione che stava invece cercando di evitare.

Insieme alla lotta è opportuno anche continuare a informare ed educare gli utenti. L'unica ragione per cui lo spamming cresce e prolifera è che, evidentemente, c'è gente che abbozza, rispondendo, visitando i siti o acquistando i prodotti pubblicizzati. Ignorare i messaggi fastidiosi è l'utopia che può liberarci da essi. Fortunatamente esistono molte organizzazioni anti-spam che forniscono informazioni soprattutto per i meno esperti. Queste organizzazioni offrono anche numerosi strumenti. Alcune di esse sono tanto attive nella lotta contro lo spamming, che a volte degenerano in una guerra radicale contro chiunque non sia totalmente d'accordo con le loro tesi.

### **1.3. Struttura della memoria**

Dopo questa introduzione, nel secondo capitolo propongo dapprima una serie di definizioni, poi quella scelta come base per questo lavoro. Sempre nello stesso capitolo descrivo i messaggi di spam dal punto di vista del contenuto e affronto la questione della differenza tra lo spamming in Rete e quello fuori dalla Rete. Il capitolo si conclude con una breve panoramica sulla parentela tra l'e-mail marketing e lo spamming, parentela che si rivelerà scomoda per l'e-mail marketing.

Nel terzo capitolo vengono fornite alcune basi tecniche sul sistema di posta elettronica, elementari ma indispensabili per comprendere i capitoli successivi. Il quarto capitolo presenta una panoramica storica del fenomeno, partendo da Usenet e da alcuni casi celebri, arricchita da alcune mie riflessioni personali sull'etica. Vengono anche precisate dettagliatamente le ragioni per cui lo spamming è considerato un problema serio.

Nel quinto capitolo si torna a trattare la tecnica, ma questa volta descrivo il modo in cui gli spammer inviano milioni di messaggi per volta e spiego come ottengono gli indirizzi dei destinatari. Presento anche due esempi di spammer molto attivi.

I due capitoli seguenti (sei e sette) affrontano il problema della lotta allo spamming. Dal lato legale fornisco una panoramica sullo stato della legislazione in alcuni Paesi, dopo aver riflettuto sull'opportunità e l'utilità di leggi che regolino il fenomeno. Dal lato tecnico descrivo alcune strategie di difesa adottate da utenti e provider. Non è ovviamente possibile elencare tutti i metodi di lotta, anche perché gli spammer inventano continuamente nuovi modi per trarre profitto dall'invasione delle nostre caselle di posta.

L'ultimo capitolo descrive il test condotto per un anno servendomi delle caselle di posta che TI-EDU mi ha messo a disposizione. Non si tratta di dati rappresentativi perché la quantità di messaggi analizzata è una goccia nel mare, né posso pretendere di paragonare questo studio alle analisi fatte da alcune aziende che, grazie ai sistemi installati presso grossi provider e aziende, possono produrre statistiche mensili sulla base di milioni di messaggi di spam. Sono però dati di prima mano che posso fornire.

#### **1.4. Ringraziamenti**

Vorrei ringraziare il professor Fiorenzo Scaroni per i suoi suggerimenti e i suoi consigli; l'ingegner Mario Gay (responsabile di TI-EDU) per i suoi commenti e per il supporto tecnico; il dottor Simonotti della Sertel s.r.l. e i suoi collaboratori, Maurizio Cavalletti e Davide Airaghi, per l'aiuto nell'estrazione dei dati; tutti coloro che lottano contro lo spamming e gli altri abusi, per rendere Internet un posto migliore.

## 2. Definizione

Il problema della definizione di spamming non è così semplice come potrebbe sembrare a prima vista. Innanzitutto, vorrei distinguere spamming e spam: con **spam** si intende il messaggio di posta elettronica non richiesto, inviato a molti indirizzi. Con **spamming** si indica il fenomeno nel suo complesso. Tuttavia, questa distinzione non è sempre usata in modo tassativo: talvolta si usa spam anche per indicare il fenomeno. Gli **spammer**, invece, sono coloro che inviano i messaggi di spam.

In rete sono reperibili altre denominazioni e definizioni:

- junk e-mail, e-mail spazzatura (generica, non necessariamente riferita a Internet);
- Unsolicited Commercial E-mail (UCE), che evidenzia la natura commerciale o pubblicitaria dei messaggi;
- Unsolicited Bulk E-mail (UBE), mette in primo piano l'invio di massa (bulk = massa);
- SPAM: Stupid People Advertising Message.

Finora non sono stati fatti molti sforzi per trovare una definizione precisa, ma si è mantenuta una certa ambiguità. Questo potrebbe essere successo perché gli spammer hanno dimostrato una grande inventiva nel trovare nuovi modi per effettuare invii di spam e quindi un termine vago era preferibile a un termine preciso ma non flessibile. Ora che il problema viene affrontato più seriamente da parte della comunità Internet e delle istituzioni, è necessario definire con precisione e completezza il fenomeno. Il primo passo per eliminare lo spam è capire cos'è.

Il termine spam è usato spesso in modo impreciso ed è causa di incomprensioni e ambiguità. Come spesso si sente dire a proposito della pornografia: «Non la posso definire, ma la riconosco quando la vedo». Gli usi errati del termine si incontrano frequentemente nei gruppi di discussioni da parte di qualche nuovo frequentatore della rete, ma non solo, oppure sui media tradizionali. Ho sentito spesso etichettare come spam gli off-topic (OT), quando in realtà con off-topic si indicano i messaggi fuori tema in una mailing list<sup>1</sup> o in un forum dedicato ad uno specifico argomento.

Oggi il termine spamming indica un fenomeno ampio che si presenta in molte forme diverse fra loro. Per questo motivo esistono più definizioni non sempre coerenti. Alcune di esse

---

<sup>1</sup> **Mailing list**: forum di discussione che corrisponde a un indirizzo e-mail, al quale gli iscritti possono mandare messaggi che verranno ricevuti da tutti gli altri iscritti.

definiscono solo un aspetto del fenomeno, altre sono solo troppo vaghe. Ho cercato di trovare una definizione che identificasse con precisione il fenomeno, ma abbastanza generica per poter essere usata senza che gli spammer possano aggirarla facilmente.

Il dizionario inglese Merriam-Webster, nella sua versione web OnLine, fa risalire il termine al 1994 ed etimologicamente indica l'origine ad uno sketch dei Monty Python<sup>2</sup>. La definizione è questa:

«spam (sostantivo): e-mail non sollecitato solitamente commerciale spedito a un grande numero di indirizzi.»<sup>3</sup>

Come vedremo, la definizione che adotterò sarà abbastanza simile.

## 2.1. Alcune definizioni

Ho iniziato la mia ricerca dal Jargon File, il popolare dizionario degli hacker<sup>4</sup> curato da Eric Raymond.

Questa la definizione completa:

«Spam/spammare:

[1] mandare in tilt un programma inserendo un'eccessiva quantità di dati in un buffer di dimensione fissa;

[2] inondare un gruppo di discussione con messaggi irrilevanti o inappropriati. Si può fare con messaggi preparati per l'occasione (per esempio chiedendo "Cosa ne pensate dell'aborto?" in soc.women). Spesso viene fatto in cross-posting. Ciò coincide con comportamento del troll, termine più specifico che sta diventando più comune;

[3] spedire molti messaggi identici o quasi identici separatamente a un gran numero di gruppi di discussione Usenet. Più precisamente, questo viene detto ECP, Excessive Cross-Posting;

[4] bombardare un gruppo di discussione con copie multiple di un messaggio. Più precisamente, questo viene detto EMP, Excessive Multi-Posting;

[5] spedire una gran massa di messaggi non richiesti identici o quasi identici, specialmente contenenti pubblicità. Il termine viene usato specialmente quando gli indirizzi e-mail sono

---

<sup>2</sup> **Monty Python**: popolare gruppo comico di registi e attori inglesi.

<sup>3</sup> **Merriam-Webster**, <http://www.m-w.com/dictionary.htm> (consultato il 23 agosto 2002).

Versione originale nell'allegato 12.1.

<sup>4</sup> **Hacker**: secondo il Jargon File: uno che ami programmare, e a cui piaccia essere bravo a farlo.

stati raccolti dal traffico di rete o da basi di dati, senza il consenso dei legittimi proprietari. I sinonimi includono UCE e UBE;

[6] qualsiasi grande e fastidiosa quantità di output.

Le ultime definizioni sono diventate più usate da quando Internet si è aperta alle persone meno esperte di tecnologie e per la maggior parte delle persone i significati 3, 4 e 5 sono quelli principali. Tutti e tre i comportamenti sono considerati un abuso della rete e sono quasi universalmente una ragione per chiudere l'account e-mail dell'origine o la sua connessione di rete. In questi significati il termine spam è diventato un termine di mainstream, ma senza il suo significato originale folcloristico - c'è apparentemente un mito diffuso tra gli utenti secondo cui spamming sarebbe ciò che accade versando lattine di Spam in un ventilatore. Hormel, i produttori di Spam, hanno pubblicato una dichiarazione sorprendentemente chiarificante sull'uso in internet.»<sup>5</sup>

In inglese, il termine “spam” sembra usato più spesso come verbo, almeno nelle definizioni di Raymond. In italiano si usa come nome, mentre in qualità di verbo si usa “spammare”, anche se non è molto bello.

Come lo stesso Raymond ammette, sembra che al giorno d'oggi il termine spam sia usato soprattutto negli ultimi sensi. Trovo particolarmente corretti i significati 3, 4 e 5, perché distinguono ciò che è lo spamming sui gruppi di discussione (Usenet<sup>6</sup>) da quello effettuato via e-mail. Lo **Usenet Spamming** è un termine generico che racchiude la definizione di ECP (Excessive Cross Posting: l'invio di molti messaggi identici o quasi identici separatamente a un grande numero di gruppi di discussione) e quella di EMP (Excessive Multiple Posting: l'invio di copie multiple di uno stesso messaggio a uno stesso gruppo). In questa memoria mi occuperò di Usenet Spam solo in modo marginale. Per **E-mail Spamming** si intende invece l'invio in massa per posta elettronica di messaggi identici o quasi identici, non richiesti, in particolare contenenti pubblicità. Il termine spamming è usato con questo significato soprattutto quando gli indirizzi e-mail dei destinatari sono stati prelevati in qualche modo senza il consenso del destinatario.

Oggi la definizione 1 («mandare in tilt un programma inserendo un'eccessiva quantità di dati in un buffer<sup>7</sup> di dimensione fissa») è poco usata, per la 2 («inondare un gruppo di discussione con messaggi irrilevanti o inappropriati...») si usa il termine “trolling”, nel senso di “provocare”. La 6 («qualsiasi grande e fastidiosa quantità di output») è un'estensione delle

---

<sup>5</sup> Eric Raymond, *Jargon File*, <http://www.tuxedo.org/~esr/jargon/> (consultato il 17 luglio 2002). Versione originale nell'allegato 12.1.

<sup>6</sup> **Usenet (gruppi di discussione o newsgroup)**: sistema di conferenze su Internet per discussioni pubbliche, forum, sulla quale si pubblicano articoli o post.

<sup>7</sup> **Buffer**: spazio di memoria in cui vengono riposti i dati in attesa di essere elaborati.

precedenti e, come evoluzione, possiamo considerarne l'uso fatto dall'Open Directory Project. Qui lo spam è definito così:

«Lo spam capita se pagine identiche vengono presentate alla stessa categoria più volte, se un sito è presentato alla stessa categoria più volte, se un sito è presentato a diverse categorie inappropriate o se la presentazione viola in altro modo le nostre Policy di Presentazione o danneggia l'ODP (Open Directory Project). »<sup>8</sup>

In Internet si trovano una quantità incredibile di definizioni. Eccone alcuni esempi.

Julian Haight, di SpamCop<sup>9</sup> definisce lo spam così:

«Per me lo spam dev'essere:

1. non sollecitato (non l'ho richiesto), e
2. automatico (lo stesso email è stato spedito a migliaia di persone in una sola volta.»<sup>10</sup>

Yahoo Italia, nelle pagine di supporto on-line, propone questa definizione:

«Lo spam è qualsiasi messaggio o annuncio che, a prescindere dal contenuto, viene inviato a più utenti che non hanno specificatamente richiesto tale email.

Può anche essere rappresentato da annunci multipli dello stesso messaggio inviati a Newsgroup o server di discussione e che non sono relativi al tema in oggetto. Altri termini comuni per lo spam presenti su Internet sono UCE (Unsolicited Commercial Email) e UBE (Unsolicited Bulk Email) e corrispondono alla stessa definizione di spam.

Gli individui che inviano spam sono generalmente persone che hanno acquistato o raccolto liste di indirizzi e-mail. Quindi, procedono all'invio di messaggi da diversi indirizzi verso ogni area del Web.»<sup>11</sup>

Fighters4web<sup>12</sup>, che riporta in italiano i testi del sito anti-spam spam.abuse.net, dopo aver definito la natura dello spamming ponendo l'accento sulla molteplicità delle copie e sulla natura

---

<sup>8</sup> **Open Directory Project**, *Open Directory Editorial Guidelines: spamming*, <http://dmoz.org/guidelines/spamming.html> (consultato il 17 luglio 2002). Versione originale nell'allegato 12.1.

<sup>9</sup> Si veda il capitolo 7.2.6.

<sup>10</sup> **Julian Haight**, *On what type of email should I (not) use SpamCop?*, <http://spamcop.net/fom-serve/cache/14.html> (consultato il 6 agosto 2002). Versione originale nell'allegato 12.1.

<sup>11</sup> **Yahoo Help**, *Che cos'è lo spam?*, <http://help.yahoo.com/help/it/mail/spam/spam-02.html> (consultato l'8 agosto 2002).

solitamente commerciale dei contenuti, identifica la differenza tra lo spam in Usenet e spam in e-mail.

Brad Templeton, presidente della Electronic Frontier Foundation (EFF<sup>13</sup>) pone l'accento sull'origine dei messaggi. Afferma inoltre che lo spam è un problema a causa della sua quantità: un solo messaggio di spam ogni tanto non è un problema. Inoltre classifica lo spam come un messaggio e-mail che soddisfa tutti e tre i criteri seguenti:

«Definisco l'abuso dell'e-mail come messaggi che rispondano a tutti e tre questi criteri:

1. Non è sollecitato
2. È parte di un "invio di massa"
3. Il mittente è estraneo al destinatario. (Il destinatario non ha mai avuto alcun contatto consapevole con il mittente.)»<sup>14</sup>

I primi due criteri si trovano in molte altre definizioni, mentre il terzo è più raro. Templeton sostiene che il 99% dello spam ricevuto soddisfa questi criteri, il resto è trascurabile. Il terzo punto può sembrare ragionevole soprattutto riguardo ai singoli individui: se una persona che conosco mi manda spam, posso chiederle di smettere. Le organizzazioni (o le aziende) non incorrono in spamming, secondo questa definizione, quando mandano messaggi ai loro membri. Ma la cosa non è così semplice: io posso comunicare il mio indirizzo di posta elettronica a un'azienda per certi scopi, ma l'azienda può abusarne per mandarmi pubblicità che non desidero. Questa obiezione viene contrastata da Templeton affermando che sono pochissime le aziende e le persone, in tutto il mondo, con cui normalmente si ha una relazione di qualche tipo. Quindi lo spam proveniente da esse è poco e non può costituire un problema. Inoltre, se sono in relazione con un'azienda che si comporta in questo modo, ho un certo controllo della situazione in quanto posso contattare le persone interessate. Nella definizione che ho scelto e che illustro nel prossimo capitolo, ho lasciato questo aspetto alle parole "non sollecitato". Come vedremo, esse vengono precisate definendo esplicitamente cosa si intende per "non sollecitato" e lasciando implicito ciò che invece è sollecitato. Questo rispecchia la prassi della nostra giurisprudenza che indica ciò che è vietato fare, non ciò che è permesso. In questo modo non si

---

<sup>12</sup> **Scott Hazen Mueller** (trad. Giulio Pipitone), *What is spam?*,

<http://www.fighters4web.com/pagine/mirror/What%20is%20spam.htm> (consultato il 17 ottobre 2002).

<sup>13</sup> **EFF**: organizzazione attiva nella difesa dei diritti degli utenti (<http://www.eff.org>).

<sup>14</sup> **Brad Templeton**, *Essays on Junk E-mail (Spam)*, <http://www.templetons.com/brad/spume/> (consultato il 24 ottobre 2002).

rischia di punire un innocente. Il terzo criterio della definizione di Templeton è pericoloso perché non pone il destinatario al riparo da abusi perpetrati da qualcuno con cui è in relazione.

La caratteristica comune di molte definizioni che si possono trovare in rete oggi è che lo spamming è un disturbo di livello e continuità tali da ostacolare la possibilità di comunicare. Tutte queste definizioni sono fatte dal punto di vista di chi si trova a dover pagare per lo spamming.

## 2.2. La definizione scelta

Una definizione breve, che restringe l'ambito di azione e identifica il fenomeno come inteso oggi, è quella trovata presso Infinite Monkeys & Company<sup>15</sup>. Credo che il significato più comune del termine spam, al giorno d'oggi, rientri quasi sempre in questa definizione. Io ho scelto proprio questa definizione come riferimento perché mi sembra al tempo stessa precisa ma non troppo restrittiva.

«Lo spam su Internet consiste di uno o più messaggi non sollecitati (1), spediti o affissi come parte di un insieme più grande (2) di messaggi, tutti aventi sostanzialmente lo stesso contenuto (3).»<sup>16</sup>

La definizione è firmata da ottanta persone (imprenditori, giornalisti, programmatori, consulenti e analisti informatici, sviluppatori, amministratori di sistema) tra cui: Ronald F. Guilmette, primo firmatario e presumibilmente autore; Julian Haight, di SpamCop, e George W. Mills, della EuroCAUCE (European Coalition Against Unsolicited Commercial Email), solo per citarne alcuni.

L'autore di questa definizione ha avuto l'accorgimento di precisare alcuni punti, per evitare malintesi.

(1) **Non sollecitati.** È importante capire cosa costituisce una esplicita sollecitazione alla comunicazione elettronica e cosa no. Una tale sollecitazione è decisa consapevolmente da parte di chi riceverà la conseguente comunicazione elettronica.

---

<sup>15</sup> **Infinite Monkeys & Company** (<http://www.monkeys.com>) è un'azienda americana specializzata nel design e nello sviluppo di sistemi informatici di sicurezza.

<sup>16</sup> **Infinite Monkeys & Company**, *Spam defined*, <http://www.monkeys.com/spam-defined/definition.shtml> (consultato il 16 luglio 2002). Versione originale nell'allegato 12.1.

Le persone intelligenti che non hanno motivazioni finanziarie, politiche o religiose per fare altrimenti dimostrano generalmente di essere in grado di capire cosa costituisce una sollecitazione esplicita e cosa no. Tuttavia, chi ha una motivazione per ignorare il buon senso e la cortesia ha ripetutamente tentato di stirare la definizione di “sollecitazione” oltre il limite accettabile. Per capire cosa si intende, segue una lista di esempi di cosa non costituisce una sollecitazione esplicita a ricevere messaggi di massa:

- una visita a un sito web non è una sollecitazione ad altre comunicazioni dirette dal gestore del sito al visitatore;
- la trasmissione di un messaggio elettronico a un singolo o a un forum pubblico (un gruppo di discussione Usenet, una chat room o un canale IRC<sup>17</sup>) non costituisce una sollecitazione a mettere l’indirizzo del mittente in una lista che verrà usata per l’invio di massa di messaggi, a meno che l’intento del messaggio originale non sia chiaramente quello, e a meno che non vengano prese precauzioni per assicurarsi che il mittente della richiesta sia in effetti il proprietario autorizzato dell’indirizzo e-mail, a cui i messaggi di massa verranno inviati;
- mettere o far mettere il proprio indirizzo e-mail in qualsiasi spazio pubblico (una pagina web, un gruppo di discussione Usenet, un sistema di bollettini o una banca dati di registrazione di domini accessibile pubblicamente) non costituisce mai una sollecitazione a partecipare come ricevente in invio di messaggi di massa, a meno che tale pubblicazione (o informazione per il contatto) non sia accompagnata da una esplicita sollecitazione in questo senso. La pubblicazione di informazioni di contatto non è, di per sè, una sollecitazione all’invio di messaggi di massa;
- l’esistenza di un forum di discussione pubblico non costituisce una sollecitazione a mandare messaggi che fanno parte di un processo di spamming, a meno che il proprietario di tale forum non abbia esplicitamente incoraggiato lo spamming su quel forum;
- una sollecitazione a partecipare in un tipo particolare di invio di massa (per esempio: la richiesta di ricevere una certa newsletter<sup>18</sup> o partecipare a una certa mailing list) non costituisce una sollecitazione a ricevere altri invii di massa, nemmeno da parte dello stesso mittente;

---

<sup>17</sup> **IRC** (Internet Relay Chat): sistema disponibile su Internet dall’inizio degli anni Novanta per conferenze on-line in tempo reale.

<sup>18</sup> **Newsletter**: messaggio di posta elettronica periodicamente inviato a una lista di destinatari, i quali ne hanno richiesto (e confermato) la sottoscrizione.

- la sollecitazione a ricevere un invio di massa può essere fatta solo da parte di chi effettivamente riceverà le comunicazioni e in nessun caso da parte di qualcun altro per conto dell'interessato.

(2) **Insieme più grande**. Non esiste un limite minimo di messaggi identici sotto al quale non si parla più di spam. Qualsiasi insieme di due o più messaggi aventi sostanzialmente lo stesso contenuto che non sono stati sollecitati dai riceventi possono essere classificati come spam.

(3) **Stesso contenuto**. I giudici di una corte suprema americana hanno formalmente definito lo spam:

«Il termine “spam” è generalmente riferito alla posta elettronica di massa non sollecitata (o “posta spazzatura”), che può essere sia commerciale (come ad esempio una pubblicità) che non commerciale (come ad esempio uno scherzo o una catena di lettere).»<sup>19</sup>

I giudici hanno considerato solo una parte dei significati, se ci atteniamo al Jargon File, ma è importante che abbiano individuato i due aspetti chiave dello spam, e cioè l'esistenza di più copie e la natura di comunicazione non sollecitata.

## 2.3. Contenuti

### 2.3.1. Categorie

La definizione di spamming è ampia e non tiene conto del contenuto del messaggio. Tuttavia, i messaggi di spam che circolano per la Rete hanno dei contenuti ricorrenti. La proposta di classificazione qui presentata serve a dare un'idea dei contenuti più frequenti. I dati provengono da Brightmail, un'azienda che produce software anti-spam. Grazie ai suoi sistemi analizza circa cinque milioni di attacchi al mese e su questa base ha definito le categorie e prodotto il grafico che riporto in questo capitolo. Viene spesso citata quando si parla di statistiche sullo spamming.

Di seguito la tabella delle categorie:

<b>Adulti</b>	Messaggi che si riferiscono a prodotti o servizi destinati a maggiorenni.
Esempi	Pornografia, annunci personali, ricerca di relazioni.
Esempi di soggetti	“Instantaneously Attract Women” “Watch Me Free On Webcam.”

<sup>19</sup> Infinite Monkeys & Company, *Spam defined*, op. cit. Versione originale nell'allegato 12.1.

	“Looking for Love, Romance or Friendship?” “Frage.”
<b>Finanziari</b>	Messaggi che contengono riferimenti o offerte relative a denaro, azioni o altre opportunità finanziarie.
Esempi	Investimenti, crediti, immobiliari, prestiti.
Esempi di soggetti	“Have you checked your personal credit reports recently?” “Get Cash, No Equity Required! Apply Today?” “We WILL Help You To Succeed With Wealth Builders”
<b>Prodotti</b>	Messaggi che pubblicizzano o offrono beni e servizi generici.
Esempi	Servizi di investigazione, abbigliamento, cosmetica.
Esempi di soggetti	“Flat Rate Long Distance” “Winter Clearance Leather Blowout Sale” “Buy 1, get 2 FREE Inkjet Cartridges” “Get your Free satellite TV system now”
<b>Internet</b>	Messaggi che pubblicizzano o offrono beni o servizi relativi a Internet o ai computer in generale.
Esempi	Webhosting, web design, spamware, prenotazione domini, virus.
Esempi di soggetti	“High Speed Internet Access is Here!” “Get 80,000 Direct Email Leads A Month!!”
<b>Spirituali</b>	Messaggi concernenti servizi religiosi o spirituali oppure messaggi atti a reclutare nuovi adepti.
Esempi	Astrologia, indagini di tipo psicologico, organizzazioni religiose.
Esempi di soggetti	“Free Psychic Readings” “Get 72 hours of Unlimited LIVE Psychic Readings” “The Truth About Your Power”
<b>Truffe</b>	Messaggi che propongono o pubblicizzano attività fraudolente o volutamente equivoche, o che conducono alla partecipazione in attività fraudolente.
Esempi	Investimenti nigeriani, schemi piramidali.
Esempi di soggetti	“Urgent Business Letter” (tipico nella truffa nigeriana) “Money in the Mail” (truffa del “diventa milionario in un anno”) “University Diplomas” (falsi diplomi in università non accreditate)
<b>Svago</b>	Messaggi che offrono o pubblicizzano premi, riconoscimenti o attività di svago scontate.
Esempi	Offerte di vacanza, casinò online, giochi.
Esempi di soggetti	“Update Now for Your Florida Vacation!” “Collect \$150 Free Chips!” “Free Cruise Certificate#243694” “Free CASINO hotel rooms & Money to Play with!”
<b>Salute</b>	Messaggi che offrono o pubblicizzano prodotti o servizi in relazione alla salute, spesso di dubbia efficacia.
Esempi	Farmaci, trattamenti medici, rimedi naturali, viagra.
Esempi di soggetti	“Online Consultation and Prescription Ordering” “Turn back your body's biological clock with ABC Oral Spray” “Breakthrough Skin Resurfacing Facial...” “Enlarge your penis. “
<b>Altro</b>	Altri tipi di contenuti che potrebbero essere, per esempio: <ul style="list-style-type: none"> <li>• elettorali: messaggi che pubblicizzano attività politiche;</li> <li>• false newsletter: le vittime vengono iscritte a loro insaputa a una o più newsletter o presunte tali. Le informazioni contenute nelle newsletter molto spesso non interessano i destinatari. Ogni newsletter riporta anche messaggi pubblicitari. Disiscriversi è difficile, nonostante quanto spesso riportato sulle newsletter stesse: si viene ignorati oppure il servizio non è attivo.</li> <li>• Joe Job: Si tratta di uno spam generico, ma fatto con lo scopo di danneggiare una specifica azienda. Per far ciò lo spammer riporta il nome e l'indirizzo dell'azienda in questione così da infangarne il nome.</li> </ul>

Tabella 1: categorie di spam secondo Brightmail

Il grafico con le analisi di Brightmail<sup>20</sup>:

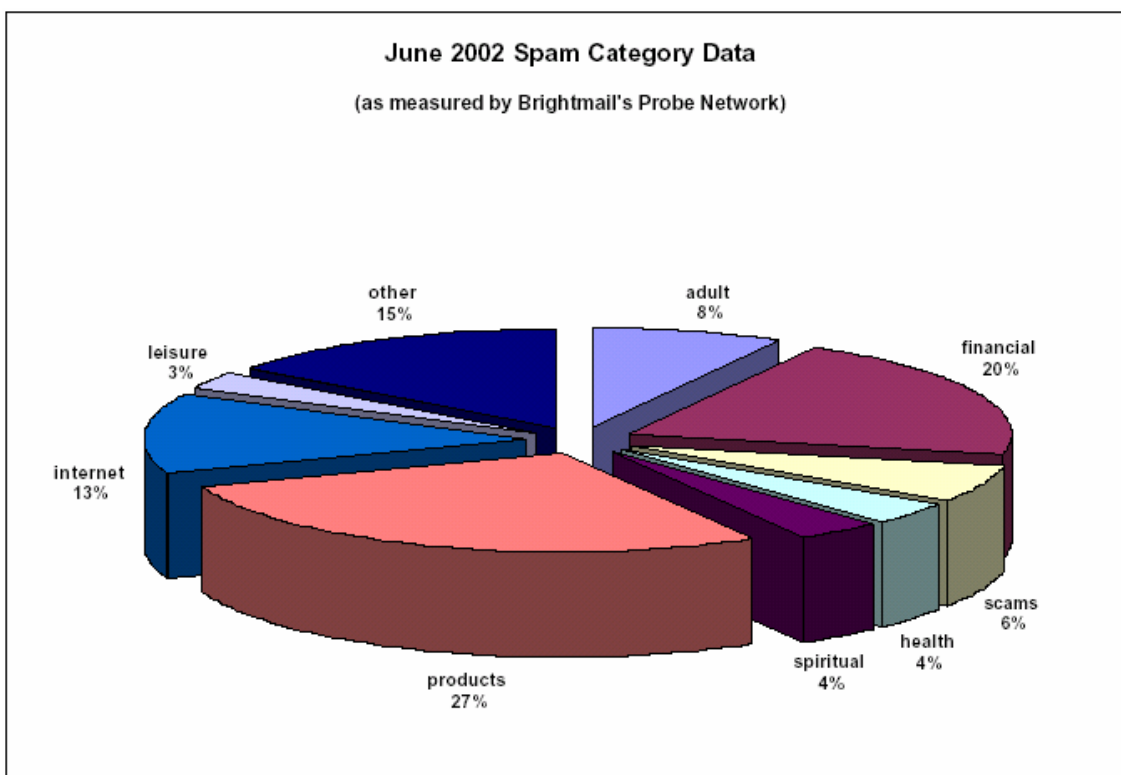


Figura 1: categorie di spam secondo Brightmail

Come si può vedere, la maggior parte dei messaggi di spam è di tipo commerciale e pubblicizza prodotti, servizi finanziari o servizi su Internet. Un'altra categoria importante è quella relativa alla pornografia ("adult"). Di solito questi messaggi pubblicizzano siti o servizi a pagamento. Si potrebbe dedurre che quasi il 70 % di messaggi di spam sia di tipo commerciale.

Secondo i dati di Brightmail sull'evoluzione dello spamming lo spamming è in crescita più o meno costante.

### 2.3.2. Truffe e fenomeni simili allo spamming

A proposito delle truffe che giungono via spamming, un documento<sup>21</sup> della Commissione Federale del Commercio americana (FTC) classifica dodici truffe tipiche. Tra le più comuni vi sono sicuramente quelle relative a opportunità di business miracolose. Spesso questi affari fanno

<sup>20</sup> Fonte: [http://www.brightmail.com/pdfs/0702\\_spam\\_definitions.pdf](http://www.brightmail.com/pdfs/0702_spam_definitions.pdf) .

<sup>21</sup> **Federal Trade Commission**, *FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email*, <http://www.ftc.gov/bcp/online/pubs/alerts/doznalrt.htm> (consultato il 15 luglio 2002).

capo a sistemi piramidali, illegali in molti Paesi. Questi sistemi, definiti anche Make Money Fast (MMF), Multi Level Marketing (MLM) o schema di Ponzi<sup>22</sup>, invitano a partecipare a un sistema di vendita di prodotti o servizi che funziona attraverso dei rappresentanti (“referrer”): chiunque può essere rappresentante dell’azienda produttrice e vendere i prodotti direttamente, basta comprare l’apposito kit iniziale. Il guadagno arriva quando il rappresentante convince altre persone a vendere per lui, incassando percentuali dai subalterni. I prodotti o i servizi, di solito, non esistono neppure e l’azienda guadagna attraverso la vendita del kit, mentre i vari livelli di rappresentanti sono alla disperata ricerca di subalterni, spammando la rete in lungo e in largo. Altre volte il gioco si riduce allo scambio di pochi soldi, che vengono mandati a una lista di persone, poi si aggiunge il proprio nome e si manda il messaggio ad altre persone.

Esistono poi alcuni fenomeni che non sono spamming, ma vi somigliano o comunque vengono messi in relazione allo spamming. Talvolta, all’inizio vi è un messaggio di spam tradizionale, che viene poi inviato da qualcuno ad alcuni destinatari, i quali a loro volta lo rinviavano ad altri destinatari. Questo schema è spesso detto catena di Sant’Antonio<sup>23</sup>, con contenuti di vario tipo. Il risultato è che si viene a creare una reazione a catena di spedizioni ad amici e conoscenti. Spesso nelle intenzioni di chi origina il messaggio non c’è scopo di lucro, ma in alcuni casi dietro a questi messaggi si nasconde una vera e propria truffa.

Questi meccanismi sono interessanti perché hanno una diffusione locale, perlomeno inizialmente. Pur non essendo vero e proprio spamming, il traffico generato è notevole e può congestionare alcuni server di posta elettronica. Ecco alcuni esempi: messaggi umanitari, netstrikes (scioperi in Rete), petizioni, segnalazioni di siti, allarmi relativi a virus o di altro genere, barzellette. I più divertenti sono sicuramente quelli relativi alle bufale (“hoax”), ma alcuni hanno dei risvolti odiosi quando trattano storie di persone con malattie rare e mortali che cercano aiuti. Questo tipo di messaggi sfrutta la credulità innata dell’essere umano. Le situazioni descritte a volte sono reali, ma più spesso sono inventate o non più attuali. Quando

---

<sup>22</sup> Carlo Ponzi nacque a Parma nel 1882. Divenne famoso perché, dopo essere emigrato negli USA nel 1903, “inventò” uno schema di finanziamento piramidale che gli permise di raccogliere nel 1920 circa 15 milioni di dollari. La promessa era quella di pagare ai creditori il 50% di interessi in soli 45 giorni. Non c’era un investimento reale dietro alla richiesta di finanziamento, L’idea alla base del sistema era questa: comprare francobolli internazionali nei Paesi in cui costavano meno e rivenderli dove costavano anche 5 volte di più. Ponzi fu in grado di pagare i primi creditori raccogliendo i soldi da quelli successivi. Il passaggio di soldi continuò fino a quando l’ammontare di interessi da pagare non superò le entrate da nuovi finanziamenti. In pochi giorni la piramide crollò e circa 40 mila persone persero i loro soldi. Come risultò dai libri contabili durante quella frenetica attività di raccolta di fondi e pagamento di interessi Ponzi aveva comprato 2 francobolli.

<sup>23</sup> La leggenda popolare narra che Sant’Antonio invitava chi riceveva una buona azione a farne cinque, per sdebitarsi.

coinvolgono aziende ignare, queste subiscono un danno economico e d'immagine. Spesso sono in circolazione per anni, quindi si possono rintracciare pagine web di spiegazioni.

## 2.4. Lo spamming fuori dalla Rete

La definizione di spam data dice che lo «spam su Internet consiste di uno o più messaggi non sollecitati, spediti o affissi come parte di un insieme più grande di messaggi, tutti aventi sostanzialmente lo stesso contenuto.»

Come si nota, si precisa con le parole «su Internet» l'ambito nel quale è applicabile la definizione. Ma possiamo trovare qualcosa di simile allo spamming anche al di fuori della Rete, nel mondo reale.

Gli americani usano da tempo l'espressione junk mail per indicare la carta inutile che invade la cassetta della posta. Anche nel nostro Paese siamo abituati a ricevere buste di vario genere provenienti da aziende, associazioni di carità, partiti politici e altro. Ma i fenomeni simili allo spamming non si limitano a questo: capita di ricevere telefonate che ci informano su prodotti o servizi oppure per sondaggi dai temi più disparati.

La nuova frontiera è il sistema di messaggistica sui telefoni cellulari GSM (SMS). Si tratta di una novità degli ultimi anni e per il momento è ancora di difficile definizione.

Non ritengo opportuno far rientrare questi fenomeni nella categoria spamming perché non si tratta di questioni legate a Internet e alla posta elettronica. Inoltre, nonostante alcune somiglianze, sussiste una sostanziale differenza: nel caso dello spamming su Internet i costi vengono sopportati dal destinatario e dagli intermediari (per esempio gli Internet Service Provider<sup>24</sup>) e solo in minima parte dal mittente, mentre nel mondo reale quest'ultimo deve inevitabilmente affrontare dei costi economici e di tempo non indifferenti. Nel caso della posta cartacea, è necessario pagare la stampa e la spedizione; nel caso delle telefonate a casa, i costi sono nel personale addetto alle telefonate e nelle telefonate stesse.

Questo è un limite naturale all'esplosione di questi fenomeni, limite che nel caso dello spamming in Internet non esiste. Un ulteriore limite, riguardante le telefonate, deriva dal fatto che i sistemi di telefonia sono gestiti da un'organizzazione in grado di ricostruire il percorso della comunicazione. Abusi estremi vengono quindi perseguiti.

Si sente parlare anche di spamming via SMS, ma mi sembra troppo presto per definire con precisione il fenomeno e le sue conseguenze. I limiti naturali sono il costo dell'invio e il fatto che esista la possibilità, da parte delle compagnie telefoniche, di rintracciare il mittente.

---

<sup>24</sup> **Internet Service Provider (ISP o semplicemente provider)**: azienda che offre servizi su Internet, tipicamente connettività, indirizzi di posta elettronica, hosting, housing... Può offrirla a utenti finali (privati o aziende) o ad altri intermediari.

Oltretutto sembra che lo spamming via SMS dipenda in una certa misura dall'atteggiamento delle compagnie telefoniche. Se queste decidessero di limitarlo (per imposizioni legali o a seguito della pressione dei propri clienti) i mezzi tecnici probabilmente ci sarebbero. Mezzi tecnici che invece non esistono (o sono limitati) nel caso di Internet.

La questione della pubblicità via fax merita una nota a parte. Anche questo mezzo di comunicazione è stato utilizzato in passato per inviare pubblicità non richiesta. Il mittente deve sopportare i costi delle telefonate, ma parte dei costi (la stampa) ricade sul destinatario. Il destinatario subisce anche dei costi indiretti rilevanti: la linea resta occupata e l'apparecchio è quindi inutilizzabile. Inoltre, nel caso di invii ripetuti da parte dello stesso mittente o in quello di invii provenienti da mittenti diversi in tempi ravvicinati, l'apparecchio può esaurire la carta o l'inchiostro e risultare così inutilizzabile per ricevere altri fax.

Per questa ragione i legislatori di molti Paesi hanno tutelato chi possiede un apparecchio fax limitando l'uso di questo strumento per invii di questo tipo. Tale legislazione viene spesso usata come base per contrastare anche lo spamming come inteso da noi, cioè quello via posta elettronica. Anche nel caso del fax, inoltre, è relativamente semplice risalire al mittente che si trova, con ogni probabilità, nello stesso Paese: se si trovasse all'estero le tariffe per le chiamate sarebbero molto alte costituendo un limite naturale di una certa importanza.

## **2.5. Lo spamming è uno scomodo parente dell'e-mail marketing?**

Lo spamming non è e-mail marketing, e l'e-mail marketing non è spamming. Nonostante questo, a prima vista le due cose possono essere considerate vicine. In realtà si tratta di una parentela lontana e non biologica, dovuta più che altro al fatto che molti messaggi di spam sono pubblicità.

In questo capitolo vorrei chiarire cos'è l'e-mail marketing e come un'azienda può sfruttare la posta elettronica per fare pubblicità senza cadere nella trappola dello spamming. Alcune aziende, infatti, hanno abboccato a offerte di spammer senza scrupoli e si sono messe nei guai con la legge e con il provider. Ora che la cultura di Internet è un po' più diffusa questo capita più raramente, ma bisogna comunque stare in guardia: le opportunità di Internet possono trarre in inganno. Il vantaggio che fa più gola è che i destinatari sono raggiungibili grazie alla posta elettronica a costo zero in tutto il mondo. Ma ci sono svantaggi e inconvenienti di cui bisogna tenere conto.

Lasciando agli esperti di marketing l'onere di approfondire il tema del contenuto del messaggio di una campagna di e-mail marketing, vorrei solo proporre alcune brevi riflessioni: la comunità Internet misura la serietà dell'advertiser anche in base al contenuto della pubblicità.

Fraasi del tipo «Le nostre ricerche indicano che lei è interessato al nostro prodotto», anche se sono la verità, sono state spesso usate a sproposito dagli spammer e quindi sono da evitare. In Rete è possibile imbattersi in alcune organizzazioni che aiutano gli advertiser nell'organizzazione di campagne pubblicitarie via e-mail. Esistono anche agenzie pubblicitarie specializzate nell'e-mail marketing o, più in generale, nell'Internet marketing, e-marketing, direct marketing o in qualsiasi altro modo lo si voglia chiamare.

Alcune aziende si sono specializzate nella redazione e spedizione di newsletter con vario contenuto informativo. È possibile, solitamente, sponsorizzare la newsletter inserendo alcune righe di pubblicità sopra o sotto le informazioni richieste dall'utente.

### **2.5.1. Definizione e particolarità dell'e-mail marketing**

L'e-mail marketing consiste nel realizzare strategie di marketing utilizzando la posta elettronica come canale di comunicazione con il cliente attuale e potenziale<sup>25</sup>. L'uso dell'e-mail come mezzo di marketing comporta il rischio di venire accusati di spamming, con danni incalcolabili per l'immagine aziendale: gli spammer suscitano un vero e proprio odio negli utenti della comunità Internet e un'accusa di spamming (anche infondata) compromette la credibilità sul mercato della pubblicità. Ricordo, infatti, che le qualità aziendali conquistate nel mondo reale con duro lavoro, su Internet non contano (quasi) nulla: reputazione, affidabilità, onestà, integrità sono da costruire di nuovo partendo da zero. Un comportamento ineccepibile in Rete mette al riparo da informazioni sbagliate e fuorvianti diffuse da terzi più o meno intenzionalmente. I danni, inoltre, potrebbero non essere limitati all'immagine dell'azienda o dell'agenzia di pubblicità, ma potrebbero avere altri risvolti legali; in più, alcuni provider tagliano la connettività anche sulla base di pochi sospetti.

Molta cautela nell'uso della posta elettronica per il marketing non significa però rinuncia completa: Internet è un'opportunità di business troppo importante. L'e-mail marketing è possibile, tanto che alcune associazioni anti-spam pubblicano consigli per le aziende che desiderano praticarlo. Esse si basano sul principio che Internet non è gratis per nessuno, soprattutto per l'utente. Pertanto chi fa pubblicità deve evitare di far ricadere sui destinatari finali costi che questi non hanno liberamente scelto. In altre parole, non bisogna mai mandare pubblicità a chi non l'ha espressamente richiesta. Questo semplice principio garantisce una convivenza ottimale tra la comunità Internet e chi desidera fare pubblicità, l'advertiser.

Un altro aspetto da tenere in considerazione sono le leggi che regolano il mercato pubblicitario: esse non sono uguali in tutto il mondo e l'azienda che fa pubblicità via posta

---

<sup>25</sup> **Adriana Galgano e Eugenio La Mesa**, *Definizione di Email Marketing*, <http://www.bcentral.it/emailmarketing/definizione.asp?ii=1> (consultato il 10 novembre 2002).

elettronica può violarne qualcuna senza volerlo. Per questa ragione è nell'interesse dell'advertiser stesso che i destinatari della pubblicità siano in qualche modo qualificati: chi pubblicizza servizi finanziari d'alto reddito non desidera che tale messaggio vada a un gruppo di bambini. Purtroppo gli indirizzi e-mail da soli non forniscono informazioni utili a questo, nemmeno sul Paese d'origine.

### **2.5.2. Un indirizzario onesto: compilazione e manutenzione**

La parte di un piano di promozione via posta elettronica che ci interessa riguarda la compilazione della lista di destinatari. L'advertiser deve conoscere il suo pubblico, e il modo migliore per farlo è quello di raccogliere informazioni di prima mano, direttamente dai destinatari interessati a ricevere pubblicità. Per farlo può, per esempio, sfruttare una pagina web per farsi mandare l'indirizzo e-mail e altre informazioni tramite un form. Il destinatario deve essere informato su quali dati vengono raccolti e per quale scopo. Se i dati vengono forniti per altri scopi, per esempio per l'iscrizione a servizi web ai quali è collegata una newsletter pubblicitaria, deve essere possibile iscriversi ai servizi senza ricevere la newsletter pubblicitaria. Questa situazione dovrebbe essere quella proposta mentre la ricezione della newsletter pubblicitaria dovrebbe essere una scelta consapevole che richiede un'azione esplicita. In molti Paesi le leggi sulla raccolta di dati personali stanno mutando. L'advertiser deve tenersi informato ed essere estremamente prudente: nel dubbio, meglio lasciar perdere.

Non è consigliabile né saggio acquistare liste di indirizzi da terzi, a meno che non si tratti di aziende specializzate la cui fama è nota e verificabile. Altrimenti, non è possibile conoscere con precisione il metodo di raccolta dei dati: molte liste in circolazione sono state compilate con metodi poco etici, a volte addirittura sfruttando liste di persone che hanno espresso l'intenzione di non ricevere pubblicità. Non si può neppure sapere se e come i rispettivi proprietari sono stati informati e a quando risale la raccolta di dati (le persone cambiano continuamente lavoro, provider,...). Di conseguenza, non è opportuno nemmeno vendere la propria lista, cosa che in alcuni Paesi è addirittura illegale.

L'iscrizione più tipica avviene tramite un form su una pagina web. Per salvaguardare la privacy dei sottoscrittori bisogna annunciare che si stanno raccogliendo i dati, dare la possibilità di rimuovere la propria iscrizione in qualsiasi momento, permettere ai sottoscrittori l'accesso ai dati per notificare i cambiamenti o correggere eventuali errori, assicurare un'adeguata sicurezza alla banca dati, evidenziare il modo per mettersi in contatto con chi raccoglie e mantiene i dati. Al momento dell'iscrizione, bisogna immediatamente richiedere una conferma al proprietario dell'indirizzo, comunicando l'indirizzo e-mail che è stato iscritto, il modo in cui è stato iscritto,

data e ora della richiesta, indirizzo IP dell'host<sup>26</sup> da cui è partita la richiesta, il nome, l'indirizzo web e e-mail dell'advertiser, le istruzioni per rimuoversi. Il tutto in un linguaggio comprensibile al destinatario medio.

In passato alcune aziende hanno proposto l'iscrizione rapida a molte mailing list, senza chiedere la conferma. In questo modo era possibile iscrivere qualsiasi indirizzo a centinaia di liste con pochi click e inoltre la procedura per rimuovere l'iscrizione era spesso complessa e poco funzionante. Per queste ragioni tali aziende sono state inondate da proteste e hanno subito denunce.

Dopo aver compilato la sua lista di destinatari per una certa comunicazione pubblicitaria, l'advertiser ha l'onere e la responsabilità di mantenerla e di verificarne costantemente i dati: validità dell'indirizzo, applicabilità del prodotto, desiderio di ricevere la pubblicità via e-mail. A tale proposito, ogni messaggio inviato deve riportare chiaramente il mittente reale e le modalità di disiscrizione, soprattutto se la lista è a basso traffico perché il destinatario potrebbe essersi dimenticato di aver sottoscritto la newsletter. Per evitare accuse infondate, è opportuno che l'advertiser tenga un archivio con tutte le richieste di sottoscrizione.

La manutenzione della lista comporta anche adeguate misure di sicurezza informatica per non farsi sottrarre i dati da pirati informatici. Per dimostrare la propria buona fede, si possono comunicare le misure adottate ai membri della lista.

## 2.6. Origine del termine spam

Concludo questo capitolo con una curiosità sull'origine del termine spam, che è nota e sembra abbastanza certa. Come già accennato, il Merriam-Webster indica come etimologia uno sketch dei Monty Python.

I primi utilizzatori di posta elettronica che si trovarono confrontati con il problema lo battezzarono con il nome commerciale di un prodotto venduto negli Stati Uniti.

SPAM (forse Spiced Pork And haM) è un tipo di carne in scatola a base di carne di maiale speziata e di prosciutto, commercializzato dalla Hormel Foods LLC. In origine era uno degli alimenti in dotazione ai militari, ma pare che sia molto buona, tanto che in rete si trovano siti di

---

<sup>26</sup> **Numero IP**: numero unico assegnato a un host su Internet. Non esistono due host con lo stesso IP. **Host**: computer (PC, server) collegato a Internet. Ha un numero IP statico (sempre quello) o dinamico (cambia se l'host viene scollegato e ricollegato come nel caso di un PC casalingo allacciato via modem).

fan appassionati (per esempio: *SPAM*<sup>27</sup> di Don Garcia e *The Amazing SPAM Homepage*<sup>28</sup> della Polly Esther Fabrique).

La carne in scatola SPAM divenne celebre in uno sketch dei Monty Python, nella serie Monty Python's Flying Circus. Nella scena, che dura un paio di minuti, un uomo e una donna entrano in una tavola calda e si siedono accanto a un gruppo di vichinghi. La cameriera elenca a voce i piatti del giorno, ma in ogni piatto c'è anche dello SPAM. Mentre parla, i vichinghi cantano con sempre più insistenza un'ode allo SPAM. I due avventori chiedono se ci sono piatti senza SPAM, ma la cameriera insiste e la parola SPAM ricorre più volte per ogni piatto. Alla fine della scena ogni parola è "SPAM" e non è più possibile comunicare.

In questo senso la parola SPAM è entrata nell'uso corrente degli utilizzatori della posta elettronica.

Tuttavia non è chiaro il momento preciso in cui la parola SPAM ha acquistato il significato attuale nella comunità Internet. Alcune fonti, tra cui Brad Templeton<sup>29</sup> fanno risalire la cosa ai primi anni Ottanta, nel mondo dei MUD<sup>30</sup>, dove veniva applicata a comportamenti diversi: "intasare" i computer con flussi di dati volutamente abbondanti, rendere inutilizzabili le banche dati con voci multiple inserite grazie a un programma e non manualmente, impedire la conversazione in chat ripetendo delle frasi in modo automatico. In quest'ultimo senso, la parola era usata anche su Relay, un antenato dell'IRC. Gli utenti di questi ambienti l'avrebbero poi utilizzata in Usenet a partire dalla fine degli anni Ottanta, ma Templeton non ha trovato tracce precise.

Il sito [www.SPAM.com](http://www.SPAM.com) è di proprietà della Hormel, l'azienda che produce la carne in scatola SPAM. La loro posizione<sup>31</sup> a proposito dell'uso del termine spam riferito agli invii di massa di posta elettronica è saggia e interessante. Viene riconosciuta l'origine del termine riferito alla scena dei Monty Python. L'azienda non si oppone all'uso del marchio che hanno registrato come slang, ma obietta quando si usa un'immagine del loro prodotto in quel senso. Inoltre chiedono che, quando non riferita alla carne in scatola, la parola spam sia scritta in minuscolo: il loro prodotto si chiama SPAM, in maiuscolo.

Per definire questa posizione, hanno preso spunto da alcune sentenze della corte federale americana, che ha stabilito dei precedenti: Star Wars può essere usato per indicare il sistema di

---

<sup>27</sup> **Dan Garcia**, *SPAM*, <http://www.cs.berkeley.edu/~ddgarcia/spam.html> (consultato il 2 agosto 2002).

<sup>28</sup> **Polly Esther Fabrique**, *The Amazing SPAM Homepage*, <http://www.cusd.claremont.edu/~mrosenbl/spam.html> (consultato il 2 agosto 2002).

<sup>29</sup> **Brad Templeton**, *Essays on Junk E-mail (Spam)*, op. cit.

<sup>30</sup> **MUD**: multi user dungeon: una sorta di ambiente virtuale dove è possibile interagire testualmente con altri utenti.

difesa americano, Cadillac può essere usato per riferirsi a qualcosa di alta qualità, Mickey Mouse per descrivere qualcosa di semplice (questi esempi hanno senso in slang americano).

Sullo stesso documento, la Hormel spiega che si oppone allo spamming e non ha mai fatto attivamente spamming, pur essendone una vittima. Il dominio SPAM.com viene preso spesso di mira da spammer che lo utilizzano per mascherare la loro provenienza, pertanto la Hormel è soggetta ad abusi maggiori rispetto ad altri.

---

<sup>31</sup> **Hormel**, *SPAM and the Internet*, [http://www.spam.com/ci/ci\\_in.htm](http://www.spam.com/ci/ci_in.htm) (consultato il 2 agosto 2002).

## 3. Basi tecniche

Vorrei spiegare brevemente come funziona la posta elettronica e quali sono i protocolli tecnici che regolano lo scambio di messaggi di posta elettronica. Lo scopo di questa introduzione tecnica è quello di essere in grado di leggere gli header di un messaggio e ricostruirne il percorso, tenendo presente quali sono le vie percorse dagli spammer.

### 3.1. Il sistema di posta elettronica su Internet

Innanzitutto, è opportuno chiarire che i computer coinvolti nella spedizione di un messaggio di posta elettronica sono molti. Oltre ai computer personali del mittente e del destinatario, vi sono i server di posta elettronica (server e-mail<sup>1</sup>). Il server e-mail del destinatario è un computer su cui risiede fisicamente la casella di posta elettronica dell'utente a cui stiamo inviando il nostro messaggio. Su di esso risiedono anche le caselle di posta di altri utenti ed è importante che sia sempre attivo e collegato alla rete. Infatti ha il compito di ricevere e conservare i messaggi degli utenti fino a quando questi non vorranno visualizzarli o scaricarli sul proprio computer personale. Questo server viene spesso chiamato server POP o IMAP, dal nome dei protocolli<sup>2</sup> che usa.

Mittente e destinatario, normalmente, dispongono di un programma detto client di posta. Tale programma è in grado di gestire i messaggi in arrivo e in partenza, di archivarli sul disco locale, di scaricare la posta in arrivo tramite il protocollo POP o IMAP e di spedire i messaggi in partenza tramite il protocollo SMTP<sup>3</sup>. Al giorno d'oggi i client di posta fanno anche altre cose: gestiscono un indirizzario, un'agenda, sanno chiamare i programmi giusti per visualizzare gli allegati e spesso sono integrati con un newsreader, per leggere i gruppi di discussione Usenet. Tra i più noti vi sono Eudora, Outlook, Pegasus. Meno noti ma non meno validi sono Pine, KMail, Netscape Messenger.

---

<sup>1</sup> **Server di posta (server e-mail)**: host connesso a Internet sul quale gira un software in grado di gestire le transazioni secondo i protocolli di posta standard (POP, IMAP, SMTP). Ospita le caselle di posta degli utenti.

<sup>2</sup> **IMAP e POP**: protocolli di ricezione per la posta elettronica. POP è usato tipicamente per connessioni via modem (ci si collega, si scarica e ci si scollega), IMAP consente un collegamento continuo.

<sup>3</sup> **SMTP**: protocollo usato per inviare la posta tramite un server e-mail.

I server di posta (POP, IMAP o SMTP) normalmente vengono gestiti dai provider. Gli ISP possono essere degli intermediari, cioè non vendono la connettività all'utente finale, ma a un'altra azienda. In questo caso, bisogna tenere presente che un ISP è sia fornitore che cliente.

Il PC del mittente non contatta direttamente il server e-mail del destinatario per recapitargli un messaggio. In teoria sarebbe possibile, ma in pratica non accade: è molto più comodo che il client sia configurato in modo da dialogare sempre con lo stesso server SMTP (normalmente quello del nostro provider). Sarà questo server a preoccuparsi di inoltrare il messaggio al server e-mail destinatario. Con questo meccanismo si evitano rallentamenti dovuti alla lontananza di rete e si semplifica la gestione da parte dell'utente finale.

Spesso i server POP e SMTP risiedono sulla stessa macchina fisica, oppure sono batterie di server (nel caso di provider di grosse dimensioni). Altre volte la rete del provider è strutturata su più livelli di sicurezza e il messaggio deve attraversare più di un server e-mail per uscire su Internet. Il risultato è sempre lo stesso: il messaggio viene inviato, ma è importante tenere presente queste particolarità quando si affronta la lettura di header.

Ecco un piccolo schema di esempio<sup>4</sup>:

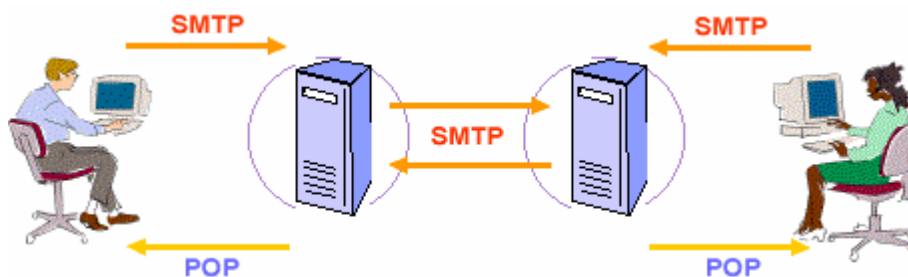


Figura 2: schema dei protocolli della posta elettronica

### 3.2. Il problema del relay aperto

Inizialmente, tutti i server di posta erano aperti a terze parti (third party relay) e accettavano messaggi da chiunque e li trasmettevano a chiunque. Questa prassi rendeva la rete Internet robusta, semplificando le configurazioni dei server, e derivava dallo spirito di cooperazione che ha pervaso la comunità Internet dell'inizio.

Da qualche tempo, i server di posta a relay aperto sono utilizzati senza scrupolo da individui che mandano un solo messaggio con una lunga lista di destinatari. In questo modo il server di posta che si sobbarca il lavoro di generare numerose copie del messaggio e di inoltrarle ai

---

<sup>4</sup> Fonte: [http://www.medasys.fr/informatique/main/solution\\_mail\\_linux.html](http://www.medasys.fr/informatique/main/solution_mail_linux.html).

destinatari non è quello del mittente. Il mittente dello spam sfrutta in questo modo il lavoro del server di qualcun altro per amplificare il suo messaggio. Inoltre, server mal configurati possono essere sfruttati per nascondere il vero mittente del messaggio.

Siccome tecnicamente non c'è più ragione per concedere il relay sul proprio server a terzi e sussiste un tale rischio di abusi, al giorno d'oggi si raccomanda di configurare i server di posta in modo che permettano il relay, ma solo a utenti o host autorizzati. Molti strumenti antispam consistono in effetti in liste di server a relay aperto, in modo che gli amministratori possano configurare i loro server di posta per non interagire con quelli elencati nelle liste. Oggi, se qualcuno volesse mantenere un server open relay, troverebbe difficilmente qualcuno disposto a interconnetterlo.

Gli ISP operano con dei server di posta intelligenti, i quali verificano che l'utente o l'host che desidera sfruttare il server per mandare la posta all'esterno del sistema sia autorizzato a farlo. È una forma di relay, ma è una pratica accettabile che permette agli utenti finali, compresi quelli in dial-up<sup>5</sup>, di usufruire del servizio.

Un server ben configurato accetta messaggi da terzi solo per i propri utenti e spedisce i messaggi a terzi solo se provenienti da macchine o utenti autorizzati. Il problema del relay aperto sussiste quando il server accetta messaggi provenienti da terzi (non autorizzati o comunque non verificati) che hanno come destinazione indirizzi esterni al dominio.

Si noti che, per accertare l'identità, non è sufficiente osservare il campo From dell'header del messaggio perché esso può essere alterato, e comunque non è ciò che viene verificato.

L'algoritmo generico raccomandato nella RFC 2505<sup>6</sup> indica come deve agire un server di posta per verificare l'autorizzazione di un host che lo contatta. Tutte le verifiche si svolgono a livello di protocollo SMTP e non hanno (quasi) nulla a che vedere con il contenuto dell'header: l'header viene costruito dal programma di posta dell'utente.

L'algoritmo prevede che inizialmente il server di posta controlli il destinatario ("RCPT To:"). Se esso è uno dei domini gestiti dal provider, allora il server accetta di fare relay, cioè consegna il messaggio.

Il passo successivo è il seguente: se la macchina che sta effettuando la richiesta ("SMTP\_Caller") è autorizzata, il server accetta di fare relay. Per questa verifica bisogna

---

<sup>5</sup> **Connessione in dial-up**: connessione via modem telefonico, la cui particolarità è il costo in base al tempo.

<sup>6</sup> **G. Lindberg**, *RFC-2505: Anti-Spam Recommendations for SMTP MTAs*, febbraio 1999, <http://www.ietf.org/rfc/rfc2505.txt> (consultato il 15 settembre 2002). Le RFC (Request For Comments) sono i documenti ufficiali di Internet, nelle quali si riportano le specifiche tecniche o altre linee guida.

decidere se affidarsi al nome di dominio (nel caso in cui ci si possa fidare del server DNS<sup>7</sup>) o controllare l'IP.

Se nessuna di queste condizioni è vera, il server deve rifiutare di fare relay. In questo caso si genera un messaggio di errore.

Propongo un esempio.

Io (*mfare@swissonline.ch*) desidero mandare un e-mail dal mio PC a casa (collegato a Internet tramite il provider Swissonline) a Mario Gay (*gay@ti-edu.ch*). Il mio programma di posta contatta il server di Swissonline, che inizia le verifiche. Con la prima, scopre che *gay@ti-edu.ch* non è un dominio gestito da Swissonline, quindi la condizione non gli permette di accettare il relay. La seconda verifica gli indica che io sono un utente autorizzato, quindi il messaggio viene inviato.

Sul lato del ricevente, il server di posta di TI-EDU (*posta.ti-edu.ch*), verrà contattato dal server di Swissonline e inizierà gli stessi controlli. Il primo gli dirà che *gay@ti-edu.ch* è un destinatario che fa parte del network TI-EDU, quindi accetterà di inoltrare il messaggio e lo depositerà nella casella di Mario Gay, il quale poi potrà leggerlo o prelevarlo tramite POP o IMAP.

### 3.3. Struttura del messaggio

Quando desidero inviare un messaggio, utilizzo il mio client di posta preferito. Il programma confeziona il messaggio e poi lo manda al mio server SMTP. Tutti i server attraverso cui il messaggio passa inseriscono alcune righe. Quando il mittente visualizza il messaggio, il suo client visualizzerà solo quelle parti del messaggio normalmente ritenute più interessanti. Per capire che strada ha fatto il messaggio (e nel caso di spam, tentare di identificare il mittente), bisogna leggere il messaggio completo di header.

Un messaggio di posta elettronica si compone di due parti: header e body. Nel body c'è il testo scritto dall'utente, l'header invece riporta le informazioni tecniche ed è la parte più interessante per risalire all'origine dello spam. Il formato del messaggio è definito nella RFC 822<sup>8</sup>. In particolare, sono definiti tutti i campi standard dell'header. Alcuni sono intuitivi e vengono visualizzati dai client di posta più comuni: From e To sono mittente e destinatario,

---

<sup>7</sup> **Domain Name System (DNS)**: sistema di server distribuito che permette la traduzione dal nome della macchina (per esempio [www.unisi.ch](http://www.unisi.ch)) al numero IP ([www.unisi.ch](http://www.unisi.ch) diventa 195.176.176.173), o viceversa.

<sup>8</sup> **David H. Crocker**, *RFC-822: Standard for the format of arpa internet text messages*, 13 agosto 1982, <http://www.ietf.org/rfc/rfc822.txt> (consultato il 15 settembre 2002).

Date e Subject sono la data di spedizione e il soggetto (definito dall'utente). Altri sono più tecnici e normalmente sono nascosti: Reply-To (il mittente definisce un indirizzo per ricevere le repliche se diverso da quello del campo From) o la riga Received, dove ogni server e-mail attraversato lascia la sua traccia. Vi è la possibilità di inserire alcune righe non standard. Queste iniziano solitamente con X- e vengono ignorate dai software che non sanno a cosa servono. La più tipica è X-Mailer, una sorta di marchio del client di posta del mittente.

Per risalire all'effettiva provenienza di un messaggio, i campi Received sono i più interessanti.

È molto importante rendersi conto che, a parte i campi Received inseriti dai server attraversati, è il client di posta del mittente a costruire tutte le altre righe. Il mittente potrebbe scrivere un programma che prepara degli header falsi, oppure potrebbe addirittura dialogare direttamente con il server SMTP, fingendosi un programma, e fornirgli indicazioni false.

Quindi, non solo gli header possono non corrispondere al vero, ma in alcuni casi non servono: i campi From e To, per esempio, servono solo agli utenti finali, non rappresentano veramente il mittente e il destinatario. Il destinatario viene specificato dal client di posta durante la transazione SMTP, quello descritto nell'header non è utilizzato per l'effettivo invio (in realtà, è usato dal programma client per dialogare con il server SMTP).

Inutile dire che lo spammer tipico, che vuole nascondere la reale provenienza del messaggio, userà queste peculiarità del protocollo per falsificare le informazioni e confondere chi cerca di rintracciarlo.

### 3.4. Panoramica su SMTP

Il protocollo SMTP serve al client di posta per inviare al server e-mail il messaggio da inviare. Vediamo rapidamente come avviene il dialogo, aiutandoci con l'invio di un messaggio immaginario ma verosimile. Le regole sono definite dal protocollo SMTP (RFC 821<sup>9</sup>). Inizialmente viene aperta una sessione sulla porta 25, segue una serie di messaggi, in alternanza tra client e server, che iniziano tutti con un codice numerico di tre cifre.

```
220 mail.swissonline.ch ESMTP server (Post.Office v3.1.2
release (PO203-101c)... ) ready
Wed, 15 Apr 1998 14:26:31 +0200
HELO mfare
250 mail.swissonline.ch
MAIL FROM:<mfare@swissonline.ch>
```

---

<sup>9</sup> Jonathan B. Postel, *RFC-821: Simple Mail Transfer Protocol*, agosto 1982, <http://www.ietf.org/rfc/rfc821.txt> (consultato il 15 settembre 2002).

```

250 Sender <mfare@swissonline.ch> Ok
RCPT TO:<mgay@ti-edu.ch>
250 Recipient <mgay@ti-edu.ch> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
From: mfare@swissonline.ch (Marco Fare)
To: mgay@ti-edu.ch
Date: Wed, 15 Apr 1998 14:24:06 +0200
X-Mailer: Gorilla 3.2 (Win95; I)
Subject: titolo del messaggio

Testo del messaggio
Marco Fare'
.
250 Message received:
19980415162853.AAA24735@mail.swissonline.ch
QUIT
221 mail.swissonline.ch ESMTP server closing connection

```

Quello che segue è un esempio di una riga Received facente parte di un messaggio realmente ricevuto presso il mio indirizzo privato (il provider è Swissonline):

```

Received: from cablecom (relay03.cablecom.net [62.2.33.103])
by mail.swissonline.ch (8.11.6/8.11.4/MSOL-2.30/21-Dec-2000)
with ESMTP id g86BsZN18423

```

La struttura della riga potrebbe cambiare a seconda dei software usati, ma più o meno è simile a questa. Vi sono molte indicazioni, ma solo alcune sono utili per identificare la provenienza. In sostanza, questa riga dice:

«Questo messaggio è stato ricevuto su mail.swissonline.ch (*by mail.swissonline.ch*), proveniente da qualcuno che si è presentato come cablecom (*from cablecom*) e che comunque aveva l'indirizzo IP 62.2.33.103, che risulta corrispondere all'host chiamato relay03.cablecom.net (*(relay03.cablecom.net [62.2.33.103])*). »

Le indicazioni (*8.11.6/8.11.4/MSOL-2.30/21-Dec-2000 with ESMTP id g86BsZN18423*) presentano la versione del software e un numero assegnato alla transazione.

Qui vi sono due cose importanti:

- possiamo ritenere questa riga affidabile solo se conosciamo il server che l'ha inserita (quello dopo il *by*). Altrimenti la riga potrebbe essere parzialmente o completamente falsa, inserita appositamente per confonderci;
- se la riga è affidabile, la parte importante è *from cablecom (relay03.cablecom.net [62.2.33.103])*. Di questo possiamo tenere conto del numero IP, perché l'ha inserito il server dopo il *by*, e il nome dell'host a cui in teoria corrisponde (relay03.cablecom.net), sempre che possiamo fidarci del server DNS. Il nome *cablecom* è quello con cui il server si è annunciato e non è detto che sia quello reale.

La riga in questione testimonia il passaggio del messaggio tra due server appartenenti alla stessa ditta: Swissonline fa parte del gruppo Cablecom.

Va detto che non sempre la riga è così pulita come quella presentata qui: gli spammer falsificano i domini, inseriscono IP a casaccio e talvolta riescono addirittura a ingannare i DNS.

È molto importante ricordare che le righe sono da leggere in ordine inverso: quella più in alto è l'ultima aggiunta.

### 3.5. Esempio di analisi di un messaggio di spam

Il messaggio analizzato è stato ricevuto il 3 agosto 2002 sul mio indirizzo presso l'USI (server e-mail: *lugano3.lu.unisi.ch*) e invitava a partecipare ai lavori di una sedicente Accademia delle Arti e delle Scienze del Nord America. Si tratta di uno spam noto, come rapidamente verificato sul gruppo di discussione *news.admin.net-abuse.sightings*.

Il Subject è: «Invitation to Be a Fellow of the North American Academy of Arts and Science.»

#### 3.5.1. Header completo

Trascrivo l'header completo del messaggio. Per facilitare la lettura, ho inserito alcune righe vuote.

```
Received: from 200.61.183.57 (customer183-
57.iplannetworks.net [200.61.183.57]) by lugano3.lu.unisi.ch
with SMTP (Microsoft Exchange Internet Mail Service Version
5.5.2650.21) id QDSX1JZG; Sat, 3 Aug 2002 09:34:04 +0200

Received: from unknown (149.89.93.47) by rly-xr02.mx.aol.com
with NNFP; Aug, 03 2002 3:26:11 AM +0300

Received: from unknown (189.234.223.231) by rly-
xr02.mx.aol.com with esmtp; Aug, 03 2002 2:16:15 AM +0600

Received: from unknown (185.176.53.24) by rly-yk05.mx.aol.com
with local; Aug, 03 2002 1:27:30 AM +0300
From: North American Academy of Arts and Sciences
<invitation@academyofartsandsciences.org>

To: Undisclosed.Recipients@mail.lu.unisi.ch

Cc:

Subject: NOT AN AD: Invitation to Be a Fellow of the North
American Academy of Arts and Sciences

Sender: North American Academy of Arts and Sciences
<invitation@academyofartsandsciences.org>

Mime-Version: 1.0
```

```
Content-Type: text/plain; charset="iso-8859-1"

Date: Sat, 3 Aug 2002 03:37:38 -0400

X-Mailer: Microsoft Outlook Express 5.00.2615.200

(...)
```

### 3.5.2. Analisi

Inizio con la verifica dell'appartenenza del dominio presente nel campo From, che tra l'altro viene ripetuto più volte nel testo del messaggio.

#### Risultati whois<sup>10</sup>

```
ACADEMYOFARTSANDSCIENCES.ORG
Administrative Contact:  NAAAS, NAAAS      naaas@mail.com
9A Potty u Budapest, na H1098 HU
Technical Contact:  NAAAS, NAAASnaaas@mail.com
9A Potty u Budapest, na H1098 HU
```

Ora estraggo manualmente le informazioni più interessanti dell'header:

#### Estratto header

```
from 200.61.183.57 (customer183-57.iplannetworks.net
[200.61.183.57]) by lugano3
from 149.89.93.47 by rly-xr02.mx.aol.com
from 189.234.223.231 by rly-xr02.mx.aol.com
from 185.176.53.24 by rly-yk05.mx.aol.com
```

Vedo a chi appartengono i vari IP:

#### Risultati di IP-whois

```
200.61.183.57
person: Martin Cabrera
e-mail: mcabrera@IPLAN.COM.AR
address: Reconquista 865 PISO 2
address: Capital Federal, Buenos Aires C1003ABQ
customer18357.iplannetworks.net:
Administrative Contact:
Nofal, Daniel dnofal@NSS.COM.AR iPlan
Salguero 2731 Suite 66
Buenos Aires, CF 1425 AR
Technical Contact:
IPLAN, NOC hostmaster@IPLAN.COM.AR NSS S.A.
Ing Butty 220 Piso 12
Buenos Aires
```

```
149.89.93.47
```

---

<sup>10</sup> **Whois**: archivi distribuiti che contengono i dati relativi ai possessori dei nomi di dominio o degli indirizzi IP.

```
Stuyvesant High School (NET-PSINET-B-89)
345 Chambers Street New York, NY 10280 US
Netname: STUY-HS
Netblock: 149.89.0.0 - 149.89.255.255
Coordinator: Rawls, Charles (CR188-ARIN) crawls@DORSAI.ORG
```

```
189.234.223.231
  inesistente
185.176.53.24
  inesistente
rly-xr02.mx.aol.com
  inesistente
rly-yk05.mx.aol.com
  inesistente
```

Analizziamo grazie a MAPS-RSS<sup>11</sup> l'IP 200.61.183.57 per vedere se risulta in qualche banca dati che raccoglie i relay aperti.

### **Analisi IP 200.61.183.57**

```
200.61.183.57 is currently on the RSS list.
```

```
This site is on our list because it is an open relay that has
transmitted spam to our users.
```

```
If you'd like 200.61.183.57 to be removed from our list,
please click here.
```

```
RSS Entry/Removal History:
```

```
Added 200.61.183.57 Sat Jun 22 05:19:35 PDT 2002 (relay)
Added 200.61.183.57 Sat Jun 22 05:19:35 PDT 2002 (relay)
Added 200.61.183.57 Sat Jun 22 05:19:38 PDT 2002 (relay)
Added 200.61.183.57 Sat Jun 22 05:19:41 PDT 2002 (relay)
```

MAPS-RSS fornisce anche informazioni più dettagliate: i messaggi che testimoniano la possibilità di usare questo server e-mail anche dall'esterno (open relay) e una copia dei messaggi di rifiuto degli avvisi che i gestori di MAPS-RSS hanno inviato agli amministratori del server incriminato.

### **3.5.3. Conclusioni sull'analisi**

Lo spammer ha utilizzato il server e-mail sull'IP 200.61.183.57, che risulta presente nella banca dati di MAPS-RSS. Questo risulta dalla prima riga Received, che è affidabile perché è stata inserita dal server e-mail dell'USI. L'IP risulta risiedere in Argentina. La seconda riga sembra indicare che un server di passaggio sia quello di una scuola di New York, mentre le righe successive riportano dati fasulli. Siccome 200.61.183.57 è un relay aperto, tutto ciò che

---

<sup>11</sup> Si tratta di un servizio anti-spam, per i dettagli si veda il capitolo 7.3.1.

segue (cioè che è stato aggiunto in un momento cronologico precedente) non può essere considerato affidabile. Quindi, questa Academy of Arts and Science, apparentemente residente in Ungheria, ha sfruttato il server e-mail aperto argentino per mandare lo spam. Gli amministratori del server e-mail argentino potrebbero essere solo negligenti, ma dalle molte segnalazioni trovate nella rete sembrerebbero più che altro compiacenti.

Per quest'analisi ho utilizzato i tool:

- Sam Spade (<http://samspade.org/>);
- Mail Abuse (<http://www.mail-abuse.org/>);
- UXN Spam Combat (<http://combat.uxn.com/>).

## 4. Storia ed etica

In questo capitolo presento alcuni aspetti storici ed etici dello spamming. Viene trattato anche Usenet perché lo spamming di massa iniziò proprio sui gruppi di discussione. Per quanto riguarda gli aspetti etici, ho cercato di riportare le opinioni correnti con obiettività, ma non si possono escludere considerazioni personali.

### 4.1. Da Usenet all'e-mail e oltre

#### 4.1.1. Alla fine degli anni Settanta

Negli anni Settanta Peter Bos, amministratore di sistema di uno dei primissimi sistemi di posta elettronica (CTSS), ha mandato il messaggio «There is no way to peace. Peace is the way.» a tutti gli utenti. Siccome gli utenti erano davvero pochi e lui era l'amministratore autorizzato a mandare messaggi collettivi, non sembra il caso di far rientrare questo messaggio nella definizione di spam.

Il primo vero messaggio di spam di cui si ha traccia risale al 1978 ed era un invito rivolto dalla DEC a tutti gli utenti di ARPANET<sup>1</sup>. La DEC presentava un nuovo prodotto: il DEC-20.

```
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, [...]
```

[segue una lista contenente decine e decine di indirizzi]

```
DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST
MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020,
2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS
HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE
DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE
```

---

<sup>1</sup> ARPANET: antenato di Internet.

DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM  
HYATT HOUSE (NEAR THE L.A. AIRPORT)  
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM  
DUNFEY'S ROYAL COACH  
SAN MATEO, CA  
(4 MILES SOUTH OF S.F. AIRPORT AT  
BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.<sup>2</sup>

Questo messaggio rientra nella definizione di spam scelta: non è sollecitato; è stato spedito a più di un destinatario e con lo stesso contenuto. In più, ha l'aggravante di essere commerciale. Si tratta comunque di spam ante litteram.

Le reazioni, non molto diverse da quelle che si trovano oggi di fronte allo spamming, furono molte. In genere, furono negative e molti chiesero ai responsabili di impedire tali abusi. Qualcuno, tra cui Richard Stallman<sup>3</sup>, sostenne che la definizione di abuso era discutibile: dov'era il confine dell'abuso? quando si poteva affermare che siccome un messaggio non era interessante non si doveva concedere il diritto di mandarlo a tutti? Stallman, che non aveva ricevuto il messaggio, disse che quando lo vide decise che era un abuso anche solo per la lunghezza dell'header. Si nota un principio importante in questa affermazione quasi goliardica: non è il contenuto che definisce l'abuso. Da notare che lo stesso Stallman afferma come già all'epoca circolavano numerosi messaggi di interesse opinabile: annunci di sistema, comunicazioni del personale (matrimoni, nascite,...).

---

<sup>2</sup> Brad Templeton, *Essays on Junk E-mail (Spam)*, op.cit.

<sup>3</sup> Richard Stallman è il fondatore del progetto GNU (<http://www.gnu.org/>) e ideologo del Software Libero.

### 4.1.2. Dagli anni Ottanta agli anni Novanta

Il 24 maggio del 1988 uno studente inviò a molti gruppi di discussione Usenet un articolo in cui chiedeva soldi per continuare gli studi. Nessuno si riferì al suo messaggio definendolo spam fino al 1996, ma nel dibattito nato intorno a quel messaggio ci si chiedeva se era un bene l'esistenza di aziende che offrivano accesso a poco prezzo.

Già negli anni Ottanta circolavano i messaggi MMF (Make Money Fast), ma erano post singoli sporadici. Per questo non sono stati definiti come spam fino quando non sono diventati veri e propri spam.

Nel 1993 un altro episodio, sempre su Usenet, irritò molti utenti. Richard Depew voleva introdurre nei gruppi di discussione la retro-moderazione (cioè cancellare i messaggi dopo che erano apparsi). All'epoca molti gruppi erano semi-moderati, ma il moderatore leggeva i messaggi in anticipo. L'idea della retro-moderazione sapeva troppo di censura, ma Depew aveva i suoi sostenitori e scrisse un software per la retro-moderazione. Il software, ARMM, aveva un bug e quando Depew lo avviò, il 31 marzo del 1993, inviò 200 volte lo stesso messaggio in *news.admin.policy*, dove si discuteva della Rete. La gente, molto irritata, lo chiamò spam. Il primo fu un certo Joel Furr. Lo stesso Depew usò la parola spam nel messaggio di scuse. Tuttavia, trattandosi di un errore accidentale, non sembra il caso di definirlo come spam.

Il 18 giugno del 1994 ogni gruppo di discussione Usenet ricevette un messaggio religioso intitolato «Global Alert for All: Jesus is Coming Soon». Il grosso problema fu che non si trattava di cross-post, ma di messaggi diversi. Il cross-post è una cosa utile se non è abusata: il messaggio è uno solo per i gruppi a cui è indirizzato e le persone lo vedono una sola volta, anche se seguono più di un gruppo a cui il messaggio è arrivato. In questo caso, si trattava di molti messaggi diversi dal contenuto identico.

### 4.1.3. Anno 1994: il fenomeno di massa

Lo spamming è diventato un fenomeno di massa nell'aprile del 1994, in occasione della lotteria per le green card. Questa lotteria è parte di un programma degli USA per distribuire i permessi di soggiorno (le green card) agli abitanti di alcuni Paesi. È necessario iscriversi e partecipare a un'estrazione. Del caso di spamming se ne occuparono alcuni giornali specializzati. Ecco come si svolse.

Il 12 aprile 1994 due avvocati di Phoenix inviarono un messaggio su Usenet nel quale pubblicizzavano un loro servizio relativo alla lotteria per le green card. Il messaggio era già stato inviato su alcuni gruppi di discussione alcune volte, ma il 12 aprile, grazie all'aiuto di un

programmatore, essi lo mandarono meccanicamente a ogni gruppo di discussione Usenet, generando migliaia di messaggi come questo<sup>4</sup>:

```
Newsgroups: comp.os.os2.bugs
From: nike@indirect.com (Laurence Canter)
Organization: Canter & Siegel
Subject: Green Card Lottery- Final One?
Date: Tue, 12 Apr 1994 05:55:50 +0000
```

Green Card Lottery 1994 May Be The Last One!  
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program giving away a certain annual allotment of Green Cards to persons born in certain countries. The lottery program was scheduled to continue on a permanent basis. However, recently, Senator Alan J Simpson introduced a bill into the U. S. Congress which could end any future lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR FIRST TIME.

The only countries NOT qualifying are: Mexico; India; P.R. China; Taiwan, Philippines, North Korea, Canada, United Kingdom (except Northern Ireland), Jamaica, Dominican Republic, El Salvador and Vietnam.

Lottery registration will take place soon. 55,000 Green Cards will be given to those who register correctly. NO JOB IS REQUIRED.

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS NOW!!

For FREE information via Email, send request  
tocslaw@indirect.com

--

```
*****
Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ 85018 USA
cslaw@indirect.com telephone (602)661-3911 Fax (602) 451-
7617
```

Laurence Canter e Martha Siegel, gli autori, erano orgogliosi del lavoro nonostante gli attacchi che subirono attraverso la casella di posta elettronica, il telefono e il fax. Il loro ISP fu sovraccaricato dalle reazioni e i giornali ne parlarono tanto che essi dichiararono di voler fondare un'azienda specializzata nella pubblicità via Usenet. Scrissero anche un libro: *How to*

---

<sup>4</sup> Brad Templeton, *Essays on Junk E-mail (Spam)*, op.cit.

*Make a Fortune on the Information Superhighway : Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services*<sup>5</sup>.

Le reazioni furono davvero molte, alcune particolarmente dure. L'Internet del 1994 aveva un atteggiamento molto meno tollerante nei confronti di chi violava le netiquette<sup>6</sup>. La stampa mondiale non si era ancora occupata del Web in modo esteso (l'avrebbe fatto, in Europa, a partire dalla fine del 1994) e i newbies, i nuovi utenti inesperti, venivano rapidamente istruiti sugli usi e costumi della Rete e assimilati tra gli utenti più esperti. Dal 1995 in poi la situazione cambiò: i newbies si moltiplicarono esponenzialmente e la maggior parte di loro non era più di estrazione accademica. Gli utenti anziani dovettero imparare a tollerare sempre più abusi dovuti più spesso a ignoranza che a negligenza. Dal 1995, la mancanza di una cultura della Rete, e di un interesse per la stessa, è un problema che affliggerà tutto Internet.

Lo spamming rovinò Usenet in modo notevole. Usenet oggi esiste grazie a software anti-spam che generano messaggi automatici di cancellazione.

Ma i problemi causati alla posta elettronica dallo spamming sono ancora maggiori: oggi la gente ha paura a mostrarsi in Rete con l'indirizzo e-mail reale. In particolare in Usenet non si usa più il proprio indirizzo e-mail, ma un indirizzo finto, inesistente o alterato. In questo modo uno dei pregi di Usenet, cioè l'integrazione con la posta elettronica, viene perso. Replicare via e-mail a un post su Usenet non è più così semplice come era stato voluto dai progettisti dei protocolli.

#### **4.1.4. Lo spamming arriva via e-mail**

A partire dal 1995 Jeff Slaton diventa il re dello spam: the Spam King. Dopo aver letto il libro di Canter e Siegel, Slaton chiese al suo provider di poter usare il suo accesso per spammare Usenet. L'ISP rispose che non era il modo corretto di fare, ma Slaton sfruttò gli ultimi giorni di abbonamento per il suo scopo: migliaia di gruppi di discussione ricevettero la sua offerta in cui metteva in vendita le riproduzioni dei modelli originali usati per la costruzione della prima bomba atomica, un documento di valore storico. Pare che molta gente le acquistò.

In seguito pubblicizzò anche il suo servizio di advertisement via spam. Slaton ha affermato di poter raggiungere fino a 8 milioni di persone i cui indirizzi sono entrati in suo possesso grazie alla raccolta su Usenet. La parte interessante del business riguarda la selettività: è possibile mandare un messaggio a mailing list o a forum con temi molto specifici. Si tratta di target advertisement, secondo Slaton ma, come egli stesso ammette, perché mandare un solo milione

---

<sup>5</sup> **Laurence Canter, Martha Siegel**, *How to Make a Fortune on the Information Superhighway : Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services*, New York, HarperCollins, 1995.

<sup>6</sup> *Netiquette: etica e norme di buon uso dei servizi di rete*. Disponibile nell'allegato 12.2.

di messaggi, quando per lo stesso costo se ne possono mandare sei milioni? Pare che la sua tattica sia molto aggressiva: grazie a trucchi o artifici tecnici sarebbe in grado di raggiungere anche le liste normalmente riservate agli iscritti o moderate.

Non mancano clienti al re dello spam: molte aziende sono attratte dall'incredibile offerta di Slaton. Agli albori dell'Internet come fenomeno di massa, nessuno si chiedeva se tale pubblicità fosse lecita o no. Nonostante ciò, nessuna azienda di grosso calibro ebbe mai a che fare con Slaton, anche se egli sostiene che ci furono contatti tramite intermediari.

Le tattiche intimidatorie che caratterizzarono la reazione della comunità Internet allo spamming di Canter e Siegel non funzionano con Slaton. Nonostante diversi ISP si rifiutino tuttora di dare un accesso a Slaton, egli continua con la sua attività sfruttando le connessioni di amici o quelle dei suoi stessi clienti. Le reazioni della Rete si sono fatte più violente: il suo numero di telefono, il nome del suo datore di lavoro e altri dati sono stati pubblicati a più riprese con l'intento evidente, anche se sempre implicito, di provocargli dei guai: fatelo licenziare, distruggete la sua credibilità come persona, punitelo per aver abusato di Internet. Ma non funziona. Slaton continua con il suo business inondando la Rete con 15 spam alla settimana, guadagnando 450 \$ a "inserzione". Nemmeno le minacce di violenza fisica lo fermano.

Il dibattito che si è creato a partire dal caso dello Spam King è interessante: molte persone hanno cominciato a riflettere sulla necessità di una legislazione che regoli la pubblicità via Internet.

#### **4.1.5. La Usenet Death Penalty**

Il ruolo degli ISP nella lotta allo spamming è cruciale. Per quanto riguarda Usenet, la comunità Internet ha notato che alcuni grossi provider non si curano dei servizi Usenet che forniscono. I gruppi di discussione vengono resi accessibili grazie a newserver installati come complemento al business principale: web e posta elettronica. Per questa ragione, alcuni utenti sono in grado di effettuare operazioni di spamming di notevoli dimensioni e prolungate nel tempo, anche quando le stesse sono contrarie alle policy dell'ISP coinvolto. Questo accade perché il provider non prende provvedimenti contro gli utenti indisciplinati.

La comunità Internet ha trovato un modo per combattere questa negligenza da parte degli ISP. La UDP (Usenet Death Penalty, pena di morte su Usenet) è un provvedimento drastico che taglia il provider negligente (e tutti i suoi utenti/clienti) fuori da Internet. Non si tratta di una punizione nei confronti degli utenti, ma nei confronti dell'ISP che non difende la netiquette. Il suo scopo principale è quello di proteggere gli utenti di altri ISP dagli abusi effettuati tramite il server incriminato.

Il suo funzionamento è semplice, ma richiede molta coordinazione. Gli ISP che aderiscono all'UDP configurano i propri server in modo da rifiutare tutti i messaggi che abbiano attraversato il server sanzionato. Se tutti i server "intorno" al server sanzionato aderiscono, questo si trova isolato e per i suoi utenti non è possibile raggiungere l'esterno. Questa limitazione è circoscritta ai messaggi Usenet diretti a gruppi non moderati. Gli utenti che utilizzano il server isolato possono comunque partecipare alle discussioni attraverso altri newsserver o attraverso gateway news-mail o news-web. Il funzionamento della posta elettronica o della navigazione su web non subisce interferenze.

La colpa dell'ISP è quella di non reprimere gli abusi per negligenza o incompetenza. In passato questa tecnica ha funzionato contro UUnet: dopo sei giorni di isolamento i vertici di questo importante provider americano cambiarono la loro politica contro lo spam.

L'UDP viene attuata dagli amministratori dei newsserver e necessita una reciproca collaborazione. In questo senso, l'UDP è un'espressione dello spirito di collaborazione della Rete e non una sua negazione in quanto il suo scopo è di favorire la discussione e non di censurarla. Un'UDP ingiustificata non verrà adottata da molti amministratori di newsserver e quindi non avrà efficacia.

Siccome l'UDP è un provvedimento drastico, essa viene attuata solo come risorsa estrema, quando tutte le altre hanno fallito. Prima di invocare un'UDP, è opportuno contattare il provider indisciplinato e cercare la sua collaborazione.

## 4.2. Lo spam è davvero un problema?

In Rete esistono molte organizzazioni dedite alla lotta, più o meno attiva, contro lo spamming. Ho cercato di scoprire quali sono i reali problemi causati dallo spamming e quanto vale la pena sforzarsi per combatterlo.

Innanzitutto bisogna dire che il problema spamming nasce dal fatto che lo spam è tanto. È inutile tacere che un solo messaggio di spam non costituisce alcun intralcio alla comunicazione. Il fatto però che un utente medio riceva verosimilmente venti o trenta messaggi di spam ogni giorno mette l'intera struttura della posta elettronica in pericolo, sovraccarica le infrastrutture degli ISP e impedisce alla gente di rivelare il proprio indirizzo e-mail con tranquillità.

Inoltre ci tengo a precisare che, pur essendo un problema con conseguenze a volte disastrose, quello dello spamming resta comunque uno dei problemi della Rete, e non certo il più grave. La sorveglianza del cittadino, le limitazioni alla libertà di espressione, le pratiche che portano alla violazione dei diritti d'autore sono solo alcuni esempi di altri problemi nati dalle nuove

tecnologie elettroniche e che affliggono Internet. Nonostante ciò, combattere lo spamming è una delle urgenze di questo periodo.

Ribadisco che l'equivalente dello spamming nel mondo reale è un problema minore: le attività pubblicitarie nel mondo reale che possiamo considerare affini allo spamming hanno dei costi alti (si pensi alla stampa o alla spedizione) che devono essere sopportati dal mittente, al contrario di quanto accade su Internet, dove a pagare sono soprattutto i destinatari e gli intermediari (provider).

La voce di chi combatte contro lo spamming è molto forte e si trovano molti documenti. Invece si trova poco materiale da parte di chi solleva obiezioni alla lotta. La ragione è che la lotta allo spamming assomiglia, per certi versi, alla caccia alle streghe. «O sei con noi o sei contro di noi!» Chi non lotta contro si vede associato agli spammer.

In ogni caso, coloro che tentano di minimizzare il problema portano alcuni argomenti ricorrenti:

- basta cancellare, non ci vuole molto tempo;
- in fondo costa poco o nulla;
- lo sforzo per lottare è troppo rispetto agli svantaggi che causa.

Sono molte le ragioni che rendono lo spamming un problema tecnico ed economico reale, e non un fastidio poco importante come in apparenza può sembrare. Molti punti sottoelencati evidenziano il fatto che i costi (tempo, spazio e denaro) non sono sopportati dal mittente. Questa è la grande differenza che distingue lo spamming dalle forme di pubblicità diretta accettate.

1. Il destinatario paga più del mittente: per cancellare i messaggi di spam bisogna prima scaricarli sul proprio PC. Normalmente questo viene fatto tramite una connessione telefonica con tariffa a tempo. Più avanti proporrò un esempio pratico.
2. Si perde del tempo a verificare il messaggio per decidere se si tratta di spam o di altro. Ciò è particolarmente vero nel caso di persone con difetti alla vista, che usano software di sintetizzatori vocali per leggere la posta. Ipotizziamo un'azienda di 50 persone, ognuna delle quali riceve cinque messaggi di spam al giorno. Supponiamo di necessitare di 5 secondi per decidere cosa fare di un messaggio. In un anno ogni dipendente spreca 8 ore nella gestione dello spam. Se ogni dipendente viene pagato mediamente 30 Fr. all'ora, risulta una spesa di 12.000 Fr. all'anno<sup>7</sup>.

---

<sup>7</sup> Sul sito <http://www.cmsconnect.com/Marketing/spamcalc.htm> è disponibile un piccolo tool per fare questi calcoli.

3. Nel caso in cui si sia connessi a Internet in modo permanente, spesso si desidera che il proprio programma di posta avvisi quando arriva un nuovo messaggio. Questa situazione è tipica nelle aziende che desiderano che i propri dipendenti rispondano celermente ai clienti che scrivono. Ogni messaggio di spam, quindi, interrompe il lavoro attirando l'attenzione.
4. I messaggi di spam intasano le caselle di posta elettronica, spesso di materiale che può essere considerato offensivo, rendendo problematico riconoscere gli altri messaggi. La frustrazione data dall'intasamento della propria mailbox danneggia lo sviluppo della posta elettronica: la paura di essere vittime degli spammer inibisce la partecipazione a forum pubblici e spinge la gente a rimuovere i propri indirizzi e-mail dai siti web. Tutto ciò rende difficoltosa la comunicazione libera. Su Usenet, lo spam crea un rumore di fondo che può anche rendere illeggibile un gruppo di discussione.
5. Anche gli intermediari (tipicamente gli ISP) pagano più del mittente:
  - a. la larghezza di banda viene occupata dalla massa di messaggi di spam. Nel caso di un ISP ciò significa fornire un servizio peggiore oppure alzare le tariffe per i clienti in modo da poter fornire più banda a questi;
  - b. i server di posta sono occupati a gestire lo spamming, quindi i messaggi legittimi subiscono dei ritardi a volte anche di giorni, se il server va in crash a causa dello spam. Nel 1997 AOL ha annunciato che tra il 5% e il 33% del tempo impiegato dai suoi server per processare i 10 milioni di messaggi che quotidianamente transitano sul network è sprecato nella gestione di spam<sup>8</sup>. Altre fonti<sup>9</sup> riportano che più recentemente AOL ha dichiarato che il 30% dei 30 milioni di messaggi quotidiani che transitano sul network AOL è spam;
  - c. i dischi degli stessi server di posta vengono riempiti da messaggi di spam. Supponiamo che un messaggio di spam occupi 10 kB e venga inviato a 10000 caselle di posta ospitate sullo stesso server di un certo ISP. Lo spazio su disco occupato è pari a 100 MB, quindi bastano 40 messaggi di spam per riempire un disco di 4 GB.
  - d. a volte il traffico eccessivo sulle reti o il carico di lavoro a cui sono sottoposti i server di posta (soprattutto nel caso di third party relay) causano veri e propri blocchi nei sistemi;

---

<sup>8</sup> **Mo Krochmal**, *Spammer Says "Uncle" To AOL*, 19 dicembre 1997, in TechWeb News, <http://content.techweb.com/wire/story/TWB19971218S0007> (consultato il 2 agosto 2002).

<sup>9</sup> **CAUCE**, *The Problem*, <http://www.cauce.org/about/problem.shtml> (consultato il 3 agosto 2002).

- e. i messaggi di errore causati dagli indirizzi errati (che spesso sono molti) occupano spazio su disco e impegnano gli amministratori dei server;
  - f. le persone addette al supporto hanno un carico di lavoro supplementare.
6. Il coinvolgimento di aziende terze può causare dei danni di immagine: tipicamente lo spammer usa mettere nel campo From un indirizzo verosimile, che sembra provenire da un provider noto. Tra l'altro, il fatto che gli spammer usino indirizzi fittizi è la dimostrazione che sanno di non essere graditi.
  7. Il danno d'immagine ricade anche su chi gestisce newsletter in modo responsabile: molto spesso gli spammer danno le indicazioni per rimuovere il proprio indirizzo dalla loro lista, ma non lo fanno. In questo modo la gente perde fiducia.
  8. I prodotti o servizi pubblicizzati nei messaggi di spam pubblicitario sono spesso di cattiva qualità, recando un danno all'intera categoria, o addirittura sono illegali.
  9. I contenuti dei messaggi di spam sono travisati con frasi del tipo "Come hai richiesto", "A seguito della tua iscrizione" eccetera. Queste pratiche sono poco leali ed eticamente discutibili.
  10. Il modo in cui lo spamming viene fatto richiede il furto, sebbene di poche risorse per volta, ed è eticamente discutibile.
  11. Il premio nobel per l'economia Ronald Coase ha stabilito che è dannoso per il mercato libero quando un business inefficiente (che non può finanziare il costo delle sue attività) distribuisce i suoi costi su un grande numero di vittime. Il pericolo sta nel fatto che, finché i costi per singolo individuo sono bassi, nessuna delle vittime è in grado di fermare il danno, che diviene virtualmente infinito per l'economia<sup>10</sup>.
  12. Lo spamming causa un degrado culturale generale a Internet.

I problemi causati dallo spamming derivano dall'imponente quantità di spamming che si sta riversando sulle caselle di posta degli utenti. Quantità che cresce ogni giorno.

In un comunicato stampa di CAUCE<sup>11</sup> del 15 maggio 2001 viene spiegata l'ipotesi secondo cui negli USA ci sono 24 milioni di piccole imprese. Se solo l'1% di queste mandasse a un certo utente un messaggio pubblicitario di posta elettronica all'anno, questo povero utente troverebbe

---

<sup>10</sup> CAUCE, *The Problem*, op. cit.

<sup>11</sup> CAUCE, *Cauce does the math - Why can't the marketing industry?*, <http://www.cauce.org/pressreleases/math.shtml>, 15 maggio 2001 (consultato il 3 agosto 2002).

657 messaggi pubblicitari al giorno. Questo calcolo evidenzia la pericolosità di una soluzione opt-out<sup>12</sup>, come vorrebbe<sup>13</sup> la Direct Marketing Association (DMA).

La soluzione dell'opt-out funzionerebbe sicuramente se l'azienda che fa pubblicità dovesse pagare: sarebbe un limite naturale.

Uno studio<sup>14</sup> commissionato dall'Unione Europea è più cauto:

1. è verosimile pensare a 300 milioni di utenti Internet in tutto il mondo per la fine del 2000;
2. uno spammer potrebbe tecnicamente mandare 100 milioni di e-mail quotidianamente;
3. 200 mittenti con tale capacità inonderebbero Internet con 20 miliardi di messaggi al giorno;
4. ogni navigatore potrebbe ricevere una media di 60 messaggi al giorno, impiegando, con le attuali tecnologie, un'ora per scaricarli.

Nella sintesi dello stesso studio è resa evidente l'ipotesi secondo cui, a livello mondiale, i costi annui dello spam per il privato sono di 10 miliardi di Euro:

«Per quanto riguarda infine la valutazione dell'onere finanziario sostenuto dagli utilizzatori di Internet, sono possibili alcuni calcoli e alcune proiezioni. Partendo dall'idea che un utilizzatore medio, che dispone di un abbonamento forfetario di 12 € per 10 ore di collegamento al mese (comunicazioni telefoniche comprese) e di un'attrezzatura standard (escluso Internet rapido) è in grado di scaricare circa 180 Kb al minuto, si ottiene un costo che può rappresentare nel peggiore dei casi fino a 30 € all'anno per lo scaricamento di una quindicina di messaggi quotidiani rappresentanti in totale tra 500 e 800 Kb. Si tratta quindi di una spesa globale assai significativa in rapporto alla scala del parco utenti di un intero paese. Sul piano mondiale e proiettandosi nel futuro, su una base di 400 milioni di utilizzatori di Internet, lo scaricamento di messaggi pubblicitari nel contesto tecnologico

---

<sup>12</sup> In breve. **Opt-in**: devo iscrivermi per ricevere. **Opt-out**: devo disiscrivermi per non ricevere. In altre parole: con il sistema opt-in, un'azienda non può mandarmi nulla a meno che non mi sia iscritto esplicitamente; con il sistema opt-out, l'azienda può scrivermi e successivamente io posso dire che non desidero ricevere nulla. Si veda il capitolo 6.2. per un discorso più approfondito.

<sup>13</sup> **Rick Lockridge**, *Congress has hard time stomaching e-mail spam*, 14 maggio 2001, in CNN.com, <http://www.cnn.com/2001/TECH/internet/05/14/spam.wars/index.html> (consultato il 3 agosto 2002).

<sup>14</sup> **Serge Gauthronet, Etienne Drouard**, *Unsolicited Commercial Communications and Data Protection (Internal Market DG – Contract n° ETD/99/B5-3000/E/96)*, gennaio 2001, [http://europa.eu.int/comm/internal\\_market/en/dataprot/studies/spamstudyen.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf) (consultato il 5 agosto 2002). Versione integrale del brano nell'allegato 12.1.

attuale corrisponderebbe a una spesa globale dell'ordine di almeno 10 miliardi di € per i soli costi sostenuti dagli utilizzatori stessi.»<sup>15</sup>

### 4.3. Questioni di etica

Nel sottocapitolo precedente ho illustrato le ragioni pratiche per cui lo spamming è un fenomeno da combattere. Legate ad esse, vi sono anche delle questioni ideologiche derivanti dalla cultura della Rete. Uno degli aspetti interessanti di Internet è che fin dalla sua prima infanzia, negli anni Settanta, le persone che se ne servivano hanno sviluppato una forte regolamentazione ideologica. In quegli anni erano soprattutto gli accademici (professori, assistenti, ricercatori, studenti) ad avere accesso alla Rete ed essi hanno trasferito alcune caratteristiche del mondo scientifico al nuovo mezzo di comunicazione. In particolare, hanno trascurato le questioni burocratiche per concentrarsi sulla collaborazione e sulla semplicità di accesso alle risorse. Questo pregio e difetto di Internet ha avuto come conseguenza che la comunità Internet ha dovuto tutelarsi dagli abusi per mezzo di una forte componente sociale. Come detto, i novizi venivano facilmente assorbiti dalla comunità ed educati a seguire le regole sviluppate quasi spontaneamente nel corso degli anni e derivanti dall'esperienza degli utenti più anziani.

Queste regole sono sintetizzate in una collezione di documenti ai quali ci si riferisce generalmente con il termine di Netiquette.

Dal 1995 in poi i nuovi utenti non sono più quasi solo esponenti accademici e sono tantissimi ogni giorno. La capacità di assorbimento è limitata e più volte gli utenti anziani rimpiangono i tempi tranquilli in cui la Rete non era di moda.

#### 4.3.1. La Netiquette

La netiquette racchiude le norme di buona educazione della Rete. Essa deriva soprattutto dall'esperienza degli utenti di Usenet o di altri forum elettronici. In essa vengono date le direttive di comportamento per poter sfruttare Internet senza infastidire gli altri utenti. Tali direttive vanno considerate come principi di buon comportamento e sono frutto dell'esperienza e della tradizione. Con il tempo essa è stata migliorata ed è entrata, in un certo modo, a far parte delle RFC. La netiquette non rappresenta la legge e non viene imposta da alcun organismo

---

<sup>15</sup> Serge Gauthronnet & Étienne Drouard, *Messaggi pubblicitari indesiderati e protezione dei dati personali, Sintesi delle conclusioni dello studio*, gennaio 2001, [http://europa.eu.int/comm/internal\\_market/en/dataprot/studies/spamsumit.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamsumit.pdf) (consultato il 5 agosto 2002).

centrale. Tuttavia è comunemente accettata, nonostante alcune critiche, e il suo rispetto viene talvolta incluso dagli ISP nelle condizioni di accesso al servizio.

Nelle mie ricerche non ho trovato una netiquette ufficiale, anche se ho trovato molte versioni identiche o quasi di uno stesso testo, che pertanto può essere considerato la netiquette. La RFC 1855<sup>16</sup> si intitola *Netiquette Guidelines* e racchiude una serie di linee guide adattabili per chi vuole scrivere una netiquette.

I messaggi di spam vengono diffusi sfruttando alcune funzionalità della Rete senza rispettare lo scopo per il quale queste funzionalità esistono e vengono pagate.

La netiquette viene spesso invocata quando si discute a proposito di spamming, ma in essa non vi è alcun riferimento esplicito. Tuttavia esistono una serie di punti applicabili allo spamming:

- Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione via posta elettronica.
- Evitare, quanto più possibile, broadcast del proprio messaggio verso molte mailing list (o newsgroups).

Nel caso di Usenet o di mailing list, la prima regola vieta i messaggi che non rientrano nell'argomento di discussione e quindi (quasi) tutti i messaggi di spam, la seconda quelli mandati a gruppi o liste diverse.

- Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito.

Questa è la regola più forte, che vieta espressamente messaggi pubblicitari o non sollecitati. È una regola molto discutibile che non è possibile applicare in ogni momento: alcuni messaggi pubblicitari potrebbero essere legittimi. Inoltre, come notato da Giancarlo Livraghi<sup>17</sup>, i messaggi indesiderati non sono sempre sgraditi.

Seguono due regole generali di principio:

- La rete è utilizzata come strumento di lavoro da molti degli utenti. Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.

---

<sup>16</sup> S. Hambridge, *RFC-1855: Netiquette Guidelines*, ottobre 1995, <http://www.ietf.org/rfc/rfc1855.txt> (consultato il 15 settembre 2002).

<sup>17</sup> Giancarlo Livraghi, *Gandalf, pensieri sulla rete e sulla comunicazione*, <http://www.gandalf.it/>.

- Qualunque attività che appesantisca il traffico sulla rete, quale per esempio il trasferimento di archivi voluminosi, deteriora il rendimento complessivo della rete.

Nel giugno del 1999 viene pubblicata la RFC 2635<sup>18</sup>, intitolata *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam\*)*. Si tratta di una serie di spiegazioni sullo spamming: cos'è, perché è un male per Internet, cosa fare se si ricevono messaggi di spam personalmente o in un gruppo, alcune indicazioni per gli amministratori di sistema e per gli ISP e alcune considerazioni di sicurezza.

### 4.3.2. Oltre le Netiquette

La Netiquette è uno strumento utile per individuare l'ideologia che regola la Rete e ci fornisce i principi generali in base ai quali il fenomeno dello spamming è negativo e va combattuto. Essa però risale ad alcuni anni fa (la RFC 1855 è del 1995) ed è necessario precisare alcuni aspetti ideologici sullo spamming e sulla lotta allo spamming.

È necessario, in primo luogo, rendersi conto che per combattere lo spamming bisogna attaccare solo chi fa spamming secondo la definizione data. Chi agisce in modi vicini alla definizione, ma non ne rientra completamente, deve essere escluso da eventuali ritorsioni o addirittura tutelato. In particolare esistono molte entità (organizzazioni, aziende, singoli gestori di mailing list, individui) che mandano messaggi a molte persone. In alcuni casi, i destinatari hanno esplicitamente sollecitato l'invio di questi messaggi. È il caso di una mailing list o una newsletter a iscrizione. In altri casi, non c'è stata sollecitazione, ma l'entità mittente è comunque legittimata all'invio di messaggi di massa. Per esempio, il gestore di una newsletter potrebbe essere intenzionato a mandare un messaggio di servizio; un'azienda comunicare con i propri clienti, o un'associazione con i propri soci; un provider potrebbe desiderare di informare i propri clienti. Nella nostra università studenti e professori ricevono messaggi dalla segreteria senza che l'abbiano chiesto. In queste situazioni, il messaggio non è stato sollecitato esplicitamente, ma il rapporto esistente tra mittente e destinatario giustifica l'invio. Naturalmente la frequenza di questo tipo di messaggi deve essere ragionevole. Nel caso di un'azienda, se essa disturba i destinatari (i propri clienti) con troppi messaggi, ne pagherà le conseguenze. Queste entità vanno tutelate, perché non fanno spamming secondo la definizione, inviano messaggi in maniera del tutto legittima.

---

<sup>18</sup> G. Lindberg, RFC-2635: *DON'T SPEW, A Set of guidelines for mass unsolicited mailings and postings (spam\*)*, giugno 1999, <http://www.ietf.org/rfc/rfc2635.txt> (consultato il 15 settembre 2002).

### 4.3.3. Etica nella lotta

Prima di iniziare a lottare contro lo spamming dobbiamo fare alcune riflessioni. La nostra società è basata sulla comunicazione aperta. Tale principio viene leso se i server e-mail vengono chiusi al relay o inseriti in una blacklist<sup>19</sup>. Per questo bisogna essere cauti prima di inserire un server e-mail nelle blacklist: potrebbe essere solo temporaneamente malfunzionante. Tuttavia, è opinione diffusa che, date le gravi conseguenze di un open relay, sia meglio chiudere i propri server e mettere gli open relay nelle blacklist anche se non spammano. Si ritiene infatti che un open relay prima o poi diventerà una fonte di spamming: gli spammer sono alla ricerca costante di server che permettano un relay aperto. Inoltre, per la stessa ragione, si possono inserire server non open ma che accettano connessioni con un'identificazione del mittente molto debole perché, nel caso in cui qualcuno modifichi leggermente gli header del messaggio (per esempio alterando il From), si comportano come se fossero open.

Ribadendo il principio della libertà della comunicazione, ogni limitazione deve essere accettata dall'utente che la deve subire. Il controllo dei filtri sulla posta in entrata da parte del provider deve essere esplicito e possibilmente la scelta deve essere lasciata all'utente, non a intermediari. Ciò non è sempre rispettato (per esempio nel caso in cui l'amministratore del server e-mail decida di affidarsi a una blacklist per limitare il traffico di spamming), ma può essere compreso visto che alcuni server non fanno altro che sparare spam. Se l'ISP intende adottare misure di protezione (l'uso di blacklist) che influenzano tutti gli utenti, dovrebbe renderlo esplicito. Inoltre il controllo dovrebbe essere distribuito: il controllo centralizzato è un pericolo per la libertà d'espressione.

La possibilità di mandare messaggi anonimi va mantenuta e garantita. La lotta allo spamming non può essere un pretesto per impedire la presenza anonima in Rete.

Un secondo principio importante, che regola la giurisprudenza della nostra società, è che è meglio non punire un colpevole che punire un innocente. Nello spamming, questo si traduce col fatto che non è possibile eliminare del tutto lo spamming, perché alcuni casi sono talmente nebulosi che sfuggono a qualsiasi definizione. In ogni caso, riceverne uno alla settimana invece che quindici al giorno è molto meno fastidioso.

Ma perché è necessario combattere contro lo spamming via e-mail? La posta elettronica sta diventando una delle risorse primarie per la comunicazione personale uno-uno, quindi va protetta con estrema cura dagli abusi. Al tempo stesso bisogna garantirne il più alto livello tenendo conto della protezione della libertà di comunicazione. In questo senso, i messaggi

---

<sup>19</sup> **Blacklist**: liste di server e-mail che per qualche ragione sono fonte di spam.

personali di posta elettronica, anche se non desiderati e noiosi, vanno protetti in ogni caso: l'abuso esiste solo quando l'invio diventa di massa.

La regolamentazione della posta elettronica non deve essere basata sul contenuto. Ciò non impedisce a un singolo utente di decidere di filtrare la posta che riceve in base al contenuto, è una sua libertà. Ma questo non deve essere generalizzato. Eventuali leggi contro lo spamming non possono comprendere il contenuto come criterio (a eccezione di casi gravi: pedopornografia, truffe eccetera, ma si va in altri ambiti). L'unico criterio possibile è la modalità di spedizione.

Nella lotta allo spamming, come in molte altre questioni riguardanti Internet, la legge è l'ultima risorsa perché soffre della giurisdizione. È impensabile che l'utente che vuole mandare un messaggio di posta elettronica si informi a priori su dove il suo messaggio arriva (o transita) e sulle leggi di quello Stato. La soluzione va cercata all'interno della comunità Internet. Inoltre, la legge potrebbe intimorire chi vuole mandare un messaggio legittimo. Se la paura di essere puniti dalla legge impedisce la comunicazione, la legge è andata troppo in là. La legge non può nemmeno considerare che gli amministratori di sistema siano responsabili per il comportamento degli utenti indisciplinati (a meno che ci siano state gravi negligenze). Non si possono mettere più limitazioni alla posta elettronica che alla posta cartacea o al telefono.

#### **4.3.4. Le opinioni degli spammer**

È raro, ma in Rete si possono trovare le opinioni di chi ha fatto spamming. Altre volte si riesce a entrare in contatto con un'azienda da cui si è ricevuto un messaggio di spam. In questo caso, l'azienda semplicemente afferma che non fa spamming. A volte queste aziende mentono. Altre volte fanno spamming, senza sapere di farlo, e questo perché, sebbene sappiano che la gente odia lo spamming, non sanno per quali motivi è odiato.

Una delle scuse più tipiche addotte per giustificare un messaggio di spam non commerciale è che si tratta di una buona causa: opere di carità o simili. Può essere vero, ma resta una buona causa nell'opinione di chi l'ha deciso. Se si trattasse di una buona causa o di un fatto importante per molte persone, la cosa arriverebbe alla gente tramite i mass media. Il problema dello spamming non è nel contenuto, ma nell'inquinamento che esso causa in Rete.

Alcune organizzazioni sostengono che non c'è altro modo per raggiungere la gente. Più precisamente, non c'è un altro modo così a buon mercato. La nostra società non permette a chiunque di possedere un canale gratis per raggiungere tutti. Nella posta tradizionale lo spamming è accettato, è vero, ma il paragone non regge: nella posta tradizionale raggiungere migliaia di persone non costa così poco.

---

Gli ideologi dello spamming sostengono che limitare lo spamming è una forma di censura e impedisce la libertà di espressione. In realtà, esistono molti modi per esprimere la propria opinione e il costo della libertà d'espressione non può essere addebitato al destinatario. Altri vedono nella pubblicità uno dei motori della nostra società e pertanto ritengono che essa sia necessaria e indispensabile e quindi bisogna garantirle degli spazi adeguati. Anche in questo caso, il costo della pubblicità dev'essere sopportato da chi la promuove, non da chi la subisce.

## 5. Le vie degli spammer

Dopo aver visto, nel capitolo 3, alcuni elementi tecnici sul sistema di posta elettronica in Internet, vorrei esaminare il modo in cui questo viene sfruttato da chi effettua spamming.

### 5.1. La spedizione

Il problema del relay aperto è uno dei più grossi, per quanto riguarda lo spamming. La breve spiegazione del capitolo 3.2 mi permette di continuare l'indagine. Ricordo che il relay aperto è un server di posta che permette a chiunque di inviare posta elettronica a indirizzi non gestiti dal server stesso.

#### 5.1.1. Tramite ISP

Lo spammer usa i server di posta di un ISP consenziente, di un ISP, cioè, che gli mette a disposizione i propri server e la propria connettività dietro pagamento o per altre convenienze. Contro provider di questo tipo si può agire legalmente (dove ci sono leggi che lo consentono) o tecnicamente, cercando di isolarlo.

L'ISP potrebbe non essere consenziente, ma potrebbe essere impossibilitato ad agire: lo spammer che usa i server di un provider direttamente è un professionista ed è molto difficile da combattere perché usa moltissimi trucchi. Per esempio, programma il proprio PC per mandare i messaggi a scaglioni, per non dare nell'occhio e non attirarsi le ire del provider. In questo caso il provider, se taglia la connettività, può trovarsi confrontato con una causa legale. Se lo spammer, invece, sfrutta in modo quasi legittimo le connessioni gratuite che si sono diffuse alcuni anni fa e le cambia ogni volta che l'ISP chiude l'account usato, diventa ancor più difficile fermarlo. Si parla di connessioni dial-up. L'ISP, in questi casi, è a sua volta vittima dello spammer in quanto quest'ultimo abusa delle risorse dell'ISP.

#### 5.1.2. Relay aperto

Come abbiamo visto, questo metodo sfrutta server mal configurati e permette allo spammer di nascondersi facendo ricadere proteste e sanzioni contro l'ISP negligente, che rischia di vedere compromesso il business e le sue infrastrutture tecniche (l'invio di centinaia di migliaia di messaggi può richiedere ore). Questa via richiede da parte dello spammer buone conoscenze informatiche e la disponibilità di server mal configurati. Per impedire questo tipo di spam è

necessario obbligare o educare gli ISP a configurare i loro server in modo che non siano aperti e isolare i server che non vengono chiusi a terzi.

Analogamente al relay aperto, esiste il problema dei proxy aperti: il meccanismo è lo stesso, ma vengono usati altri protocolli e non SMTP.

### **5.1.3. Relay multihop**

È molto simile al relay aperto, ma sfrutta server SMTP secondari. Tipicamente, infatti, le reti complesse si affidano a più server di posta, uno dei quali gestisce le comunicazioni tra interno ed esterno (smarthost). Se uno dei server secondari non è ben configurato, esso può essere sfruttato da uno spammer per inviare messaggi di spam tramite lo smarthost, che accetta di rispedirli verso l'esterno perché gli sembra che provenga da un host autorizzato. Il messaggio di spam arriva poi al server SMTP del destinatario.

### **5.1.4. No relay**

Lo spammer si connette direttamente al server e-mail del destinatario senza utilizzarne di intermedi. In questo modo può aggirare qualsiasi chiusura del relay sul server finale. Se un ISP filtrasse questo tipo di messaggi, i suoi utenti non potrebbero più ricevere alcuna posta proveniente dall'esterno. È inoltre difficile risalire all'origine perché spesso gli spammer usano connessioni dial-up volanti. Il problema è particolarmente sentito da grossi ISP che hanno molti utenti. Il costo dello spamming di questo tipo è alto anche per lo spammer (in termini di tempo soprattutto), ma è efficace e combatterlo è estremamente difficile. Per conoscere l'indirizzo di un server e-mail è sufficiente consultare i campi MX nei DNS.

### **5.1.5. Sistemi misti**

Spesso gli spammer riescono a usare una combinazione di alcuni sistemi. Per esempio, potrebbero usare il server e-mail di un ISP spam-friendly per connettersi a un open relay e, tramite quest'ultimo, allacciarsi direttamente al server e-mail di un grosso provider per spammarne gli utenti. In questo modo sono difficili da rintracciare.

### **5.1.6. Il software**

Ho cercato di scoprire quali software usano gli spammer per le loro attività. Se si effettua una ricerca con un qualsiasi motore indicando le parole "bulk mail software" o simili, si trovano decine di siti che vendono liste di indirizzi o abbonamenti per ricevere indirizzi freschi ogni settimana. Il tutto per un prezzo contenuto: 100 dollari per un CD con un milione di indirizzi oppure un abbonamento di 30 dollari alla settimana per ricevere, ogni settimana, 500.000 indirizzi freschi.

Anche il software per inviare in massa molti messaggi non è molto costoso. Prima di presentarne uno come esempio, vorrei far notare che gli spammer “grossi” (alcuni esempi sono nel capitolo 5.4) si servono di liste più costose, perché garantite da altri spammer, e di software costruito ad hoc.

Le liste e i software in vendita su siti un po’ loschi o pubblicizzati tramite messaggi di spam vengono utilizzati da piccoli spammer, quasi artigianali, ma non per questo meno dannosi.

Il software che ho trovato navigando per la Rete sembra abbastanza serio, nel senso che viene venduto per usi apparentemente legittimi e non come software per spamming: gli è stata data una maschera più rispettabile. L’azienda che lo produce si chiama Mail Utilities<sup>1</sup>.

Ecco le loro offerte:

- **Advanced Direct Remailer:** è un software in grado di mandare messaggi multipli usando una lista di indirizzi come destinatario. Agisce tramite un server e-mail interno e sfrutta al 100% la banda disponibile via modem analogico. È l’ideale per mandare spam tramite connessioni dial-up volanti. Costa 40 dollari.
- **Advanced Maillist Verify:** verifica la validità degli indirizzi e-mail presenti in una lista connettendosi ai server e-mail interessati, ma senza mandare effettivamente il messaggio. Costa 40 dollari.
- **Advanced Email Extractor:** disegnato per estrarre gli indirizzi di posta elettronica dalle pagine web o da dischi locali, sfrutta i protocolli HTTP e HTTPS. Può agire attraverso un proxy ed è molto veloce grazie alla possibilità di effettuare connessioni multiple. La versione completa costa 40 dollari, quella professionale 99.95 dollari. È possibile scaricarlo gratuitamente per un periodo di prova di 30 giorni.
- **Autoroute SMTP:** è un piccolo tool gratuito che permette di utilizzare semplicemente svariati server SMTP a dipendenza della connessione utilizzata.

Il CD-ROM completo di questi e altri programmi costa 9.95 dollari (un risparmio impressionante!). Nella sezione Press Room del sito si può leggere lo scopo per il quale questi programmi sono stati creati. L’azienda ammette che i suoi tool possono essere utilizzati per lo spamming, ma tenta di dare degli esempi di usi legittimi dei suoi programmi. Uno di questi esempi è particolarmente improbabile: viene descritta la situazione in cui qualcuno ha trovato la soluzione a un problema avanzato in un gruppo di discussione tempo prima. Per avvisare tutti i partecipanti (anche quelli che nel frattempo hanno smesso di seguire il gruppo) si possono estrarre tutti gli indirizzi memorizzati e mandare loro un messaggio.

---

<sup>1</sup> Mail Utilitites, <http://www.mailutilities.com/>.

L'azienda sostiene che questo tipo di attività non è molto diversa dal frequentare convegni, mostre e aste e raccogliere biglietti da visita per poi mandare pubblicità, offerte di lavoro o altro. Ho già chiarito<sup>2</sup> le differenze tra mondo reale e mondo virtuale. Nel caso di un biglietto da visita distribuito in una fiera o a un convegno, le eventuali telefonate o lettere pubblicitarie hanno un costo sopportato dal mittente. In più, chi distribuisce il proprio biglietto da visita si aspetta una certa pertinenza nell'uso che il ricevente farà dei dati così acquisiti.

## 5.2. Gli indirizzari

La prima domanda che l'utente inesperto si pone quando riceve un messaggio di spam è: "Come ha fatto questo tizio a procurarsi il mio indirizzo?" Procurarsi indirizzi di posta elettronica è estremamente semplice e i metodi usati possono essere diversi.

### 5.2.1. Da Usenet

È possibile, anche in modo automatico, raccogliere indirizzi sui gruppi di discussione Usenet. Infatti, nonostante il protocollo di Usenet (NNTP<sup>3</sup>) sia diverso da quello usato per la posta elettronica, esso ha molti punti in comune. Uno di questi è proprio l'indirizzo del mittente, che è quello di posta elettronica. Anche la struttura del messaggio (header e body) è molto simile.

Gli articoli Usenet possono essere esaminati uno per uno alla ricerca della riga From, nell'header. Gli archivi dei gruppi di discussione si trovano anche "tradotti" per il web (esempio: Google Groups raccoglie un archivio ventennale) oppure sui news server sparsi per il globo. Non è possibile impedire di esaminare in questo modo i gruppi di discussione, perché è lo stesso identico modo usato per leggere gli articoli normalmente. I programmi usati per questo scanning sono spesso chiamati spambot. Giulio Pipitone, gestore del sito Fighters4web (partner di EuroCAUCE<sup>4</sup>), ha pubblicato un articolo<sup>5</sup> in cui descrive un suo tentativo di costruire una lista di indirizzi partendo dai gruppi di discussione. Il programma sviluppato eseguiva questi cinque passi: apertura del server news, scaricamento di tutti i gruppi di discussione italiani, accesso sequenziale ai gruppi di discussione, apertura di ogni messaggio, salvataggio su file del campo From.

---

<sup>2</sup> Si vedano i capitoli 2 (Definizione) e 4 (Storia ed etica).

<sup>3</sup> **NNTP**: protocollo Internet usato per i gruppi di discussione (newsgroup) su Usenet.

<sup>4</sup> **Fighters4web**, <http://www.fighters4web.com/> e **EuroCAUCE**, <http://www.euro.cauce.org/>. Di queste organizzazioni tratterò nel capitolo 7.1.

<sup>5</sup> **Giulio Pipitone**, *Rapporto su situazione "prevenzione spam" sui newsgroup*, marzo 2002, <http://www.fighters4web.com/pagine/esperimenti/studiomarzo.html> (consultato il 22 ottobre 2002).

Stando a quanto descritto dall'autore, il programma è stato scritto in meno di un'ora. In due ore e trenta minuti, grazie a una connessione in fibra ottica, vengono scansionati 2367 gruppi. Può sembrare un tempo molto alto, considerando che l'equivalente per un modem analogico sarebbe di circa diciotto giorni, ma gli spammer impiegati in questo tipo di attività sfruttano connessioni veloci oppure si collegano in quelle zone dove la tariffa telefonica urbana non è fatturata a tempo.

Il file ottenuto è grande: 29 MB per un totale di 821.909 righe (potenzialmente indirizzi). A questo punto uno spammer potrebbe già utilizzarlo, senza preoccuparsi di eliminare i doppi e gli indirizzi alterati. Lo studio di Pipitone però procede e in poco tempo l'autore ripulisce il file da tutti gli indirizzi doppi, ottenendo 132.875 indirizzi. Infine vengono eliminate le stringhe di caratteri ("nospam", "toglimi",...) che alcuni utenti inseriscono nel proprio indirizzo per mascherarlo, rendendo validi circa 15.000 indirizzi con poco sforzo.

Il risultato di poche ore di lavoro è un file contenente 124.322 indirizzi, per la maggior parte validi, raccolti dai gruppi di discussione italiani.

Questo piccolo studio dimostra quanto sia semplice procurarsi indirizzi su Usenet, improvvisando una scansione dei soli gruppi di discussione italiani.

### 5.2.2. Da altre fonti

Un'altra fonte di indirizzi è il web. Le pagine web contengono molti indirizzi di posta elettronica e non è difficile scrivere degli spambot in grado di leggerli e riconoscerli, sia dal tag in cui solitamente sono contenuti ("[mfare@swissonline.ch](mailto:mfare@swissonline.ch) </a>") sia dalla loro struttura (*user@domain.tld*), sfruttando anche i siti delle organizzazioni che gestiscono i domini e che pubblicano apertamente le banche dati.

Una via sempre legata al web è quella messa in atto attraverso siti che riescono a leggere l'indirizzo immesso nei parametri di configurazione del browser. Questi siti spesso si aprono grazie a del codice javascript inserito in pagine web poco raccomandabili o in messaggi di spam precedentemente ricevuti. Con javascript è tra l'altro possibile farsi mandare un messaggio e-mail senza che l'utente se ne accorga. Lo stesso tipo di codice javascript può essere inserito in messaggi e-mail di spam che viene automaticamente eseguito dal programma di posta elettronica dell'utente. Una cosa simile può essere fatta con una richiesta di ricevuta automatica. Tornando al web, alcuni siti chiedono di inserire il proprio indirizzo in un form per ricevere una password in modo da accedere ai contenuti. Anche in questo caso, personaggi poco raccomandabili usano gli indirizzi così raccolti per fare spamming.

Vi è poi tutta una categoria di programmi di messaging: ICQ, vari tool IRC o altro, che possono venire usati dagli spammer per raccogliere indirizzi e per fare spamming. E ci sono anche modi totalmente scorretti come il cracking di sistemi per violare le banche dati.

L'acquisto di archivi di indirizzi e-mail è una pratica diffusa. Come detto, gli spammer possono acquistare CD contenenti milioni di indirizzi di posta elettronica, raccolti nei modi più disparati, per poche centinaia di dollari. Le cifre richieste possono anche raggiungere cifre molto alte se gli indirizzi sono di qualità (volontari, segmentati, selezionati,...), naturalmente con garanzie dubbie. Questi archivi vengono pubblicizzati attraverso messaggi di spam. Chi ci casca o è in malafede o è imperdonabilmente ingenuo e rischia di violare la legge.

Gli archivi venduti in questo modo sono spesso di cattiva qualità. Oltre alle operazioni di pulizia che Pipitone ha effettuato, ci sono altre ragioni per cui le liste sono inefficaci. Come si vedrà nei capitoli seguenti, continuo a ricevere spam sugli indirizzi messi a disposizione da TI-EDU, indirizzi che sono stati resi pubblici in vari modi circa un anno fa e non più usati. E sono in molti, fra cui il giornalista Giancarlo Livraghi<sup>6</sup>, che ricevono spam su indirizzi che non usano più da anni. Le liste in circolazione sono vecchie.

Lo stesso Livraghi fa notare come la maggior parte dello spam che si riceve non riguarda il destinatario: a partire dalla lingua, che è quasi sempre l'inglese, per arrivare alle offerte commerciali preparate per il mercato americano. Gli spammer non si curano della segmentazione del loro target.

A volte, per ripulire le liste, viene inviato uno spam fasullo, uno specchietto per allodole, per ottenere risposte e confermare l'esistenza di indirizzi validi di persone interessate a un certo tema. Tale operazione viene detta spamrun. Per esempio, un'azienda invia un messaggio di spam in cui annuncia che regalerà una stampante a chi risponde. Gli indirizzi raccolti dalle risposte sono esistenti e i loro proprietari sono interessati ai prodotti informatici.

### 5.2.3. Generazione automatica

È probabile che alcuni spammer generino gli indirizzi in modo automatico. Per fare ciò si servono di domini noti, come per esempio *hotmail.com* o *libero.it*, ai quali premettono una stringa (quasi) casuale. Vengono così generati migliaia di indirizzi, tra cui molti non validi. Validi o no, allo spammer non interessa: il costo di tale operazione non è molto elevato (serve solo del tempo per permettere al computer di calcolare tutte le possibilità).

La stringa casuale può essere lunga quattro, cinque caratteri, o forse di più. È improbabile che sia più lunga di dieci. Infatti, con una stringa di cinque caratteri vi sono venti milioni di combinazioni possibili, mentre con dieci le possibilità sono centomila miliardi.

Ho trovato conferma di questa idea parlando con il personale di TI-EDU e, in seguito, grazie a numerosi riferimenti in forum, siti e gruppi di discussione. Inoltre alcuni messaggi di spam ne sono una prova: quello che segue è un estratto del contenuto del campo From di un messaggio ricevuto:

mlc07@cherou.com	mlc1025@aol.com
mlc009@aol.com	mlc1053@aol.com
mlc0123@aol.com	mlc106@aol.com
mlc0358@aol.com	mlc10dan@aol.com
mlc0622@aol.com	mlc11111@aol.com
mlc069@aol.com	mlc11447@aol.com
mlc0917@aol.com	mlc011@msn.com
mlc092476@aol.com	mlc01@msn.com
mlc0970@aol.com	mlc05@msn.com
mlc100280@aol.com	mlc09@msn.com
mlc100@aol.com	mlc0@msn.com
mlc1015@aol.com	mlc10@msn.com

Tabella 2: elenco indirizzi generati automaticamente

Questi indirizzi erano nel campo Cc mescolati ad altri. Si vedono chiaramente i numerosi tentativi sul dominio *aol.com* e su *msn.com*, due fornitori di accesso molto noti in tutto il mondo. Il mio *mlc07@cherou.com* era l'unico indirizzo con il dominio *cherou.com*.

Per provare questa ipotesi ho fatto anche un piccolo test. Tempo fa, per altri motivi, ho creato un indirizzo e-mail gratuito su Bluewin. Bluewin è l'azienda appartenente a Swisscom che fornisce servizi Internet a privati (connessione e posta elettronica). Essendo un'azienda svizzera di derivazione statale ritengo poco probabile che venda gli indirizzi dei propri utenti agli spammer. L'indirizzo *mfare@bluewin.ch*, creato il 14 gennaio 2002, è stato utilizzato solo da me, per scambiarmi file con comodità. Nonostante esso non sia stato reso pubblico in alcun modo, dopo qualche mese (il 16 agosto 2002) ho iniziato a ricevere messaggi di spam. Ho quindi creato un altro indirizzo, sempre su Bluewin, ma con un nome utente complicato: *a6.c-h2.n.h-u@bluewin.ch*. Tredici caratteri senza alcuna logica. L'ho usato solo per mandare alcuni messaggi di prova. Dopo circa nove mesi dalla sua creazione, avvenuta il 19 aprile 2002, non è ancora arrivato alcun messaggio di spam.

<sup>6</sup> Giancarlo Livraghi, *Gandalf, pensieri sulla rete e sulla comunicazione*, op. cit.

Dopo questo test improvvisato, ne ho fatto uno più controllato: ho creato due indirizzi sul servizio gratuito di Hotmail. Il primo è *mimi1080@hotmail.com*, il secondo *z9\_u\_b7\_d\_b\_a@hotmail.com*. Da notare che *mimi1080* è già di per sé abbastanza complicato: sono otto caratteri e si tratta di lettere e numeri. I due indirizzi sono stati creati entrambi l'11 giugno 2002 e non sono mai stati usati se non per un paio di messaggi di test.

Dopo circa sette mesi (8 gennaio 2003), su *z9\_u\_b7\_d\_b\_a@hotmail.com* erano arrivati tredici messaggi, tutti dei servizi di hotmail e nessuno di spam. Su *mimi1080@hotmail.com* erano arrivati 1353 messaggi di spam e sedici di servizio. Il primo messaggio di spam era arrivato il 13 agosto, solo due giorni dopo la creazione dell'indirizzo. Non tutto lo spam però, probabilmente, proviene da spammer dotati di generatori automatici: è abbastanza plausibile che chi ha generato l'indirizzo l'abbia inserito in una lista che poi ha venduto o distribuito in qualche modo. Molti messaggi di spam, inoltre, provengono da server che hanno potuto connettersi direttamente ai server e-mail di Hotmail.

Tempo fa ho creato anche un indirizzo presso un altro fornitore di connettività e telefonia svizzero: Sunrise. L'indirizzo è *mfare@freesurf.ch*. Anche questo dominio è abbastanza noto perché corrisponde agli indirizzi gratuiti della Sunrise. A questo indirizzo ho iniziato a ricevere spam solo dopo molti mesi dalla sua apertura e comunque in quantità minime. Probabilmente il dominio *freesurf.ch* non è conosciuto quanto *bluewin.ch*, oppure la Sunrise ha predisposto metodi anti-spam più efficaci.

### 5.3. All'interno del messaggio, tecnicamente

La tradizione Internet consiglia che i messaggi di posta elettronica vengano scritti in formato testo per mantenere la compatibilità con il maggior numero di programmi e di piattaforme. Negli ultimi anni, però, sempre più programmi di posta gestiscono altri formati (soprattutto HTML e RTF) e moltissima gente li usa. Gli spammer se ne sono accorti e si sono subito adattati. Ormai molti messaggi di spam sono in formato HTML. Gli inconvenienti di questa situazione sono due. Innanzitutto i messaggi in formato HTML sono più pesanti di quelli in formato testo. Spesso contengono anche immagini. Inoltre, siccome molti programmi visualizzano automaticamente il messaggio, ci si espone anche ad alcuni pericoli: il codice HTML potrebbe nascondere degli script in javascript che agiscono chiamando un server remoto oppure mandando un messaggio senza che l'utente se ne accorga. Più semplicemente, le immagini visualizzate potrebbero non essere allegate al messaggio, ma richiamate dal server remoto nel momento in cui si apre il messaggio, indicando allo spammer che l'indirizzo esiste e

il messaggio è stato letto. Il link a un certo sito potrebbe essere falsato: cioè il contenuto reale del link potrebbe essere diverso da quello presentato nel testo.

In Italia, negli ultimi mesi, la situazione è ulteriormente peggiorata: dietro ad alcuni link si nascondono programmi chiamati dialer che, approfittando del fatto che la maggior parte della gente usa lo stesso sistema operativo, interrompono la connessione a Internet del modem e ne instaurano un'altra, chiamando un numero a pagamento.

## 5.4. Si guadagna?

La risposta a questa domanda non sembra difficile: evidentemente sì, si guadagna. Perlomeno, alcuni soggetti sono riusciti a guadagnare, anche molto, e questi esempi attirano persone desiderose di arricchirsi rapidamente. Un primo esempio: Steve<sup>7</sup> è un ragazzo di 32 anni che, dopo aver investito poche migliaia di dollari in attrezzature informatiche, ora guadagna 40.000 dollari all'anno. Ma Steve è uno spammer di medio livello. Piuttosto, vorrei descrivere i casi di due spammer di alto livello recentemente riportati da alcune riviste americane. È interessante notare che i protagonisti di queste storie si sono arricchiti inviando milioni di messaggi pubblicitari per conto di terzi. Il loro guadagno non deriva dalla pubblicità fatta via spam, ma dal fatto stesso di fare spam per conto di terzi. La filiera dello spamming è infatti costituita da molti attori: in basso ci sono i consumatori, le vittime, i potenziali acquirenti; a un livello alto le aziende che commissionano l'invio di messaggi. Non sono riuscito a trovare dati per sapere se fare pubblicità via spam genera realmente più affari. Verosimilmente si riesce a conquistare qualche cliente, ma nessuno si è arricchito di molto in questo modo. Il costo di questo tipo di pubblicità è però così basso che ne vale la pena, se non si considerano tutti gli svantaggi di cui si è ampiamente parlato. Infine, a metà strada della filiera, tra i consumatori e le aziende, ci sono coloro che probabilmente si arricchiscono di più: gli spammer qui descritti e i rivenditori di software per spammer e liste di indirizzi.

### 5.4.1. La regina dello spam

Da qualche mese Laura Betterly<sup>8</sup> ha avviato una piccola azienda familiare, la Data Resource Consulting<sup>9</sup>, in Florida. Ogni mese la Betterly spedisce circa 60 milioni di messaggi

---

<sup>7</sup> **Melissa Solomon**, *The Other Side*, 11 novembre 2002, in Computerworld, <http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,75736,00.html> (consultato il 28 novembre 2002).

<sup>8</sup> **Mylene Mandalindan**, *For Bulk E-Mailer, Pestering Millions Offers Path to Profit*, 13 novembre 2002, in The Wall Street Journal Online, [http://online.wsj.com/article\\_email/0,,SB1037138679220447148,00.html](http://online.wsj.com/article_email/0,,SB1037138679220447148,00.html) (consultato il 14 novembre 2002).

<sup>9</sup> **Data Resource Consulting**, <http://www.dataresourceconsulting.com/>.

pubblicitari per conto dei suoi clienti. Non si sente la regina dello spam, come talvolta viene definita, e comunque non le importa: lei fa il suo mestiere per vivere ed educare i figli. Non infrange alcuna legge, non falsifica gli header, non usa strutture tecniche o nomi di dominio senza permesso e, soprattutto, adempie alle richieste di rimozione dalle sue liste da parte di chi non desidera ricevere i suoi messaggi. Inoltre non accetta di inviare messaggi in relazione ad attività pornografiche o comunque di cattivo gusto. Il suo reddito stimato è di 200.000 dollari all'anno. Vive in una casa di 450 metri quadrati con piscina e può permettersi orari flessibili.

È la legge dei grandi numeri: su cento milioni di destinatari, la percentuale di chi è interessato alla pubblicità che arriva è sufficiente per guadagnare. Un invio è remunerativo anche se solo cento persone ogni dieci milioni rispondono. Alcune commissioni sono particolarmente vantaggiose: 35 dollari per ogni vendita di occhiali 3d, 60 per un'ipoteca, 85 per la vendita di un telefonino. Altre volte non è così. Per esempio, un'azienda intermediaria aveva commissionato un invio per pubblicizzare un concorso che aveva in palio una stampante. Per partecipare al concorso era necessario andare su un sito web e compilare un form. Il guadagno, per la Betterly, era di 75 centesimi per ogni formulario completo. Delle 500.000 persone contattate, solo 65 hanno partecipato, generando un guadagno di 40 dollari, ma le spese erano state di 250 dollari, secondo la Betterly. Se una campagna tradizionale (con invii per posta cartacea) avesse avuto un tale tasso di risposta, sarebbe stato un disastro economico.

La Betterly può contare su di una banca dati di 100 milioni di indirizzi, i cui proprietari hanno in qualche modo, anche implicito o involontario, dichiarato di voler ricevere pubblicità. Stando a quanto dichiarato, i dati sarebbero profilati: possono venire selezionati solo i piccoli imprenditori, o i golfisti o gli appassionati di musica o gli abitanti di una certa area geografica. La lista, che viene anche rivenduta, è in continua crescita tramite acquisizioni da altre liste.

Il suo provider è WorldCom, ma si basa anche su altri, perché è già successo che, a causa dei reclami, WorldCom le sospendesse l'accesso per qualche tempo. Per non irritare i diversi provider, le spedizioni avvengono in tranche di 150 messaggi.

Tra i suoi clienti non mancano le aziende che producono software anti-spam. Se qualcuno compra, la Betterly incassa il 40% del prezzo del prodotto.

Un'attenzione particolare viene riservata per la stesura del soggetto del messaggio: per fare in modo che più persone possibile lo leggano deve sembrare personale.

### 5.4.2. Il (nuovo) re dello spam

La nuova casa di Alan Ralsky<sup>10</sup> è in Virginia ed è costata più di mezzo milione di dollari. Buona parte dei 750 metri quadrati è nel seminterrato dove sono installati circa venti computer e tutte le attrezzature di rete necessarie per operare sulla linea veloce a disposizione di uno degli spammer più attivi e più odiati della Rete. Secondo Spamhaus<sup>11</sup> i responsabili del 90% dei messaggi di spam che circolano in Rete sono circa centocinquanta. Ralsky è tra i primi cinque.

Le leggi della Virginia l'hanno costretto a un accordo giudiziario con Verizon, il suo provider. Nonostante questa sembri una vittoria contro lo spamming, in realtà è una sconfitta: ora i computer di Ralsky lavorano a tempo pieno per contattare altri computer, perlopiù al di fuori degli USA, che manderanno lo spam. Usa centinaia di domini e può contare su 190 server e-mail, situati soprattutto in Asia, in grado di inviare un miliardo di messaggi al giorno. A volte succede che qualche grosso provider americano interrompa il traffico a un provider cinese a causa dello spam di Ralsky. Il provider cinese, informato dell'accaduto, esclude Ralsky, che passa rapidamente a un altro provider.

Lui dice che niente di ciò che fa è illegale. Per di più, è un business molto redditizio. Come la regina, anche questo re dello spam non tratta pornografia. Tra i suoi clienti vi sono casinò e farmacie che operano online, aziende che offrono promozioni per vacanze o prestiti finanziari.

Ha una lista di 250 milioni di indirizzi. Nei suoi messaggi ci sono le istruzioni per rimuovere la propria iscrizione e 89 milioni di persone pare l'abbiano fatto. Ralsky guadagna fino a 22mila dollari per l'invio di un singolo messaggio a tutti gli indirizzi della sua banca dati. Per monitorare le sue campagne include spesso nei messaggi del codice nascosto che comunica ai suoi server quando un messaggio viene aperto.

Pochi giorni dopo la pubblicazione dell'articolo su Ralsky, nei forum anti-spam hanno iniziato a circolare informazioni sul suo conto: indirizzo fisico, fotografia satellitare della villa, numeri di telefono. Ora Ralsky, secondo un aggiornamento<sup>12</sup> dell'articolo citato, riceve quintali di carta al giorno: cataloghi e newsletter commerciali a cui i suoi nemici l'hanno iscritto.

---

<sup>10</sup> **Mike Wendland**, *Spam king lives large off others' e-mail troubles*, 22 novembre 2002, in Detroit Free Press, [http://www.freep.com/money/tech/mwend22\\_20021122.htm](http://www.freep.com/money/tech/mwend22_20021122.htm) (consultato il 24 novembre 2002)

<sup>11</sup> Spamhaus è un'organizzazione anti-spam, trattata nel capitolo 7.3.4.

<sup>12</sup> **Mike Wendland**, *Internet spammer can't take what he dishes out*, 6 dicembre 2002, in Detroit Free Press, [http://www.freep.com/money/tech/mwend6\\_20021206.htm](http://www.freep.com/money/tech/mwend6_20021206.htm) (consultato il 18 dicembre 2002)

## 6. Spamming e legge

Lo spamming è una delle piaghe di Internet. Non è certamente la peggiore, ma i messaggi di spam in circolazione sono sempre di più e sembra che non si possa far nulla per contenerli. Vorrei fare il punto sulla situazione delle “armi” che esistono contro gli spammer. In questo capitolo mi occuperò delle questioni legali, nel prossimo presenterò alcune soluzioni tecniche a disposizioni di utenti e amministratori di sistema.

Il mondo si è accorto dello spamming. Dopo gli amministratori di sistema, si sono accorti dell’invasione le aziende, le associazioni di consumatori e infine anche i legislatori. Ma a chiedere una soluzione è soprattutto il mondo economico, spinto dal desiderio di sfruttare Internet come mezzo per la pubblicità ma confrontato con l’esigenza degli utenti di poter utilizzare la posta elettronica senza dover subire un’invasione incontrollata della propria mailbox, con gli inconvenienti che abbiamo visto. Invece l’esigenza principale delle aziende è quella di poter sfruttare la posta elettronica come mezzo pubblicitario in modo legale ed etico. Si sta cercando di definire un limite entro il quale l’azienda è legittimata ad agire e oltre il quale si sfocia nell’illegalità. Questa situazione poco chiara ha certamente influenzato molte aziende che hanno scelto di non utilizzare la posta elettronica per campagne di marketing, oppure stanno procedendo con molta cautela. Infatti le aziende più note non sono direttamente coinvolte in fenomeni di spamming, ma nemmeno praticano e-mail marketing.

Dopo aver tentato di appellarsi alla legislazione esistente, con risultati di vario tipo, gli interessati hanno focalizzato il dibattito su alcuni punti: qualsiasi legislazione deve coinvolgere almeno quella di Stati Uniti e Unione Europea. Anche in questo modo, però, è facile prevedere che il problema sarà solo spostato, e neanche di tanto: già oggi molto spam arriva da Paesi asiatici (Cina, Corea) o sudamericani (Brasile). Un altro punto importante è la necessità di trovare un vero compromesso tra le esigenze delle aziende e quelle dei consumatori. Tutte le entità coinvolte hanno capito che è necessaria una soluzione urgente che permetta legalmente di escludere i soggetti che violano la legge, garantendo l’uso confortevole della posta elettronica per gli utenti e la possibilità per le aziende di farsi pubblicità senza il rischio di incorrere in sanzioni. Una normativa a livello statunitense ed europeo sarebbe un forte messaggio anche ai Paesi esterni. Ma i dubbi ci sono e restano: per quanto possa essere ben fatta, nessuna legge è finora riuscita a condizionare Internet. La legge può essere considerata come una delle armi contro lo spamming, ma non certo la migliore.

## 6.1. Legge sì o legge no?

Prima di affrontare l'argomento vorrei proporre qualche riflessione generale sull'uso della legge nella lotta allo spamming, che tenga conto della società e delle legislazioni degli Stati democratici. I diritti fondamentali coinvolti nel problema sono la libertà d'espressione, il diritto alla proprietà privata e il diritto alla privacy. Mentre il pubblico, cioè il governo, deve agire nelle limitazioni della costituzione in merito alla libertà d'espressione, il privato (cittadino o azienda) è più libero perché può appoggiarsi alla difesa della proprietà privata. Infatti non bisogna dimenticare che Internet è una rete composta da reti prevalentemente private: il governo non possiede direttamente le dorsali nazionali. Questo significa che i proprietari possono fare (quasi) tutto ciò che vogliono sulle loro reti, ma garantire la libertà d'espressione resta una buona idea anche per i privati. Filtrare, da parte di un ISP, i messaggi in entrata per i propri clienti è illegale in alcuni Paesi e comunque è una pratica che richiede, almeno eticamente, di informare il cliente o di lasciargli la scelta. La libertà d'espressione su Internet va salvaguardata anche perché il supporto di tutti gli aspetti di Internet alla democrazia sta diventando ogni giorno più importante. Due parole anche sull'anonimato: qualcuno può sostenere che garantire l'anonimato è inutile se non dannoso. Però esso, nella nostra società libera e democratica, è un diritto e come tale va garantito.

Molte soluzioni anti-spam che possiamo utilizzare al giorno d'oggi sono in contrasto con la presunzione d'innocenza, uno dei principi fondamentali del diritto. Capita di frequente che, per educare un provider indisciplinato, si puniscano tutti i suoi utenti, anche quelli innocenti, in modo che questi si rivoltino contro il loro provider e lo costringano ad adeguarsi alle pratiche anti-spam.

Qualsiasi soluzione legale è geograficamente limitata. Per questa ragione dev'essere in realtà considerata un'ultima risorsa, dove altre soluzioni hanno fallito. Oggi non sono ancora state esplorate tutte le altre soluzioni non legali, ma la legge può, in alcuni casi, essere di supporto a queste. Quella geografica è una limitazione importante non solo perché rende difficoltoso il perseguire un abuso originato in un altro Paese, ma anche perché impone a chi scrive di adeguarsi alle leggi di chi riceve. Le leggi finora varate, soprattutto in alcuni Stati americani, non hanno fermato il problema.

Qualsiasi regolamentazione legale non dovrebbe avere come base il contenuto del messaggio, come invece vorrebbero alcuni esponenti del mondo economico. Per una società democratica è molto pericoloso permettere che la decisione sulla legalità o illegalità di un messaggio di posta elettronica sia presa in base al suo contenuto. La legge, se non si può fare a meno di ricorrere ad essa, dev'essere basata sul modo di spedizione.

Come accennato, la legge viene comunque in aiuto alla lotta contro lo spamming: molti messaggi di spam pubblicizzano frodi di vario tipo oppure hanno il mittente falso, usano domini e nomi di terzi senza autorizzazione. Alcuni fanno spamming tramite agenzie e server all'estero e poi affermano di non essere stati loro a commissionare l'invio. In breve, mentono e questo è illegale. Alcune soluzioni che verranno illustrate in seguito richiedono la cooperazione della legge. In ogni caso, va ricordato che qualsiasi tipo di lotta deve partire dalla definizione del problema e in questo senso l'appoggio legale è fondamentale.

Ma il grande vantaggio della legge lo si potrà riscontrare nella punizione degli abusi. La tecnologia, in questo caso, deve aiutare la legge fornendo le prove documentate degli abusi perpetrati dagli spammer. Infatti, lo spammer potrebbe sperare di farla franca solo quando è la sua parola contro quella di chi l'accusa. La legge deve poter disporre di uno strumento per appurare la verità e smentire lo spammer che mente, in modo che l'accusa sia fondata su prove tangibili.

## 6.2. Opt-in e opt-out

Prima di esporre gli argomenti trattati nell'ampio dibattito su una regolazione legale del fenomeno spamming, vorrei spiegare due concetti chiave: opt-in e opt-out.

### 6.2.1. Definizioni

**Opt-out** è la possibilità per il destinatario, una volta ricevuto un primo messaggio, di rimuovere la propria iscrizione dalla lista di destinatari in modo da non ricevere più altri messaggi da quello stesso mittente.

**Opt-in** è invece la possibilità di iscriversi a una lista di destinatari interessati a ricevere la comunicazione.

### 6.2.2. Implicazioni

Le definizioni dei due concetti ci portano rapidamente ad alcune considerazioni: l'opt-out sottintende l'implicito diritto di mandare un primo messaggio a una lista di destinatari per informarli della loro presenza nella lista, dando loro la possibilità di manifestare l'intenzione a non fare parte di tale lista. I destinatari devono quindi compiere un'azione concreta per non ricevere ulteriori messaggi. Una soluzione esclusivamente opt-in, invece, implica il divieto anche di un solo invio. È chi desidera ricevere i messaggi che deve richiederlo, iscrivendosi e compiendo così un'azione esplicita per riceverli.

Tra questi due estremi vi sono alcune possibilità intermedie. Per esempio, la variante opt-out può consistere in un messaggio di invito, senza iscrizione automatica alla lista. A quel punto, se il destinatario non fa nulla non riceverà altri messaggi, se invece è interessato può iscriversi. Il problema di una soluzione di questo tipo, nel contesto dello spamming, sta nella quantità dei soggetti autorizzati da questa forma di opt-out a mandare messaggi. Per esempio, se tutte le aziende svizzere (400.000 secondo il registro di commercio<sup>1</sup>) mandassero un solo messaggio all'anno agli indirizzi di posta elettronica in Svizzera, ogni utente riceverebbe un migliaio di messaggi al giorno. I numeri sono impressionanti, malgrado siano relativi alla sola Svizzera.

Vorrei aggiungere che il concetto di opt-out ha una cattiva fama perché molti spammer lo usano nei loro messaggi. Essi però non tengono conto delle richieste di rimozione dall'indirizzario (richieste che usano per confermare l'esistenza dell'indirizzo e-mail di chi risponde), quindi l'utente riceve ancora più messaggi di spam.

### 6.2.3. Il “listone” opt-out

È da considerare anche l'istituzione di liste di opt-out, cioè liste in cui chi non desidera ricevere messaggi di tipo promozionale può (deve?) iscriversi. Se ne è parlato a livello europeo, ma sono già attive alcune iniziative private. Le aziende, prima di inviare la loro pubblicità, hanno il dovere di confrontare la loro lista con quelle contenenti gli indirizzi di chi ha manifestato l'intenzione di non ricevere tali messaggi. I messaggi privati, mandati a uno o pochi destinatari, sono esclusi da tali limitazioni. Gli oppositori ritengono che non sia corretto costringere chi non desidera ricevere pubblicità (pagando) a compiere un'azione. Inoltre ci sono molti dubbi relativi alla privacy e alla sicurezza di tali liste, che dovrebbero essere per forza pubbliche o semi-pubbliche.

Una cosa simile succede in molti Paesi per la telefonia: il detentore di un numero di telefono può comunicare alla società che gestisce gli elenchi che non desidera ricevere chiamate promozionali. Le legislazioni nazionali che regolano questo tipo di liste vengono talvolta chiamate in causa quando si parla di opt-in e opt-out nello spamming. Vorrei però ricordare la differenza tra il mondo di Internet e quello fuori da Internet: le chiamate telefoniche promozionali hanno un limite naturale dovuto ai costi economici e di tempo. In più, il tutto è gestito da poche società telefoniche operanti all'interno di una giurisdizione nazionale, mentre una soluzione di questo tipo applicata a Internet dovrebbe essere sicuramente sovranazionale. E bisognerebbe prendere l'ardua decisione sulle entità a cui affidare la gestione della lista. Anche il controllo tecnico in caso di abusi, nella telefonia, è molto più efficace rispetto a quanto possibile su Internet.

---

<sup>1</sup> Ufficio federale dei registri di commercio, <http://www.zefix.admin.ch/hrweb/ita/zefix.htm> (consultato il 20 novembre 2002).

### 6.3. La tutela della privacy: TRUSTe

Il diritto alla privacy esiste ed è simile nelle legislazioni dei Paesi occidentali. Ci sono alcune differenze, anche culturali, e sul tema è in corso un animato dibattito dovuto all'invasione tecnologica degli ultimi anni e alla situazione internazionale del dopo 9/11. Il principio alla base di questo diritto è quello di proteggere la sfera privata dei cittadini.

La privacy, vale a dire la riservatezza dei dati personali, è spesso chiamata in causa quando si parla di spamming. Il collegamento tra spamming e privacy non è del tutto evidente, ma sembra che attualmente gli unici mezzi legali efficaci per contrastare il proliferare dello spamming siano quelli che si rifanno al principio della privacy. Leggi come quella svizzera (Legge sulla Protezione dei Dati) riguardano la modalità di raccolta e gestione dei dati personali, tra cui l'indirizzo di posta elettronica. Grazie alle leggi sulla privacy si intende proteggere l'indirizzo di posta elettronica dagli abusi. L'indirizzo di posta elettronica dovrebbe comunque poter essere un dato pubblico e al tempo stesso protetto dalla legge sulla privacy in relazione al principio di pertinenza, secondo cui l'uso del dato privato pubblicato è autorizzato unicamente per gli scopi per cui è stato pubblicato.

Il navigatore di Internet si trova confrontato con un problema: per poter sfruttare le possibilità messe a disposizione dalla Rete, dal commercio elettronico alla ricezione di messaggi informativi, è necessario fornire i propri dati personali. Raramente il fornitore del servizio desidera conoscere solo l'e-mail (è il caso delle newsletter di informazioni), più spesso i dati richiesti sono anche altri (per gli acquisti on-line bisogna dare nome, cognome, indirizzo e numero della propria carta di credito). Gli strumenti a disposizione del navigatore per giudicare l'affidabilità di un sito non sono molti. Ci si deve fidare di quanto raccontato nelle "Privacy policy" da chi gestisce il servizio e raccoglie i dati. Un aiuto in più viene da enti che certificano queste policy. Uno dei più importanti si chiama TRUSTe<sup>2</sup>, che si definisce un'iniziativa indipendente e non-profit il cui scopo è quello di accelerare la crescita dell'industria di Internet costruendo la fiducia dei consumatori. TRUSTe è stato fondato nel 1996, tra gli altri, dalla Electronic Frontier Foundation (EFF) ed è sponsorizzato da aziende importanti come AOL e PricewaterhouseCoopers. Il programma di TRUSTe è basato sull'autoregolazione in quanto i promotori ritengono che la regolamentazione governativa della Rete sia costosa e inefficace. Il funzionamento è semplice: TRUSTe agisce come terza parte ponendosi tra il navigatore (che dà i dati) e il fornitore di servizi (che raccoglie i dati). Il fornitore di servizi che desidera aderire al programma deve adeguarsi ai principi di privacy indicati da TRUSTe, accettando di sottostare a controlli periodici. In cambio potrà esporre sul suo sito un "trustmark", un segno di

---

<sup>2</sup> TRUSTe, <http://www.truste.org/>.

riconoscimento tramite il quale il navigatore può controllare facilmente, grazie a una chiamata ai server di TRUSTe certificata digitalmente, se l'adesione è reale. L'adesione al programma ha un costo che va dai 500 agli 8000 dollari, a dipendenza della dimensione dell'impresa.

#### **6.4. Leggi sullo spamming nel mondo**

Senza voler entrare in dettagli troppo giuridici, vorrei presentare in una panoramica la situazione delle leggi attualmente in vigore contro lo spamming.

In generale, ho notato che in Europa (Svizzera compresa) l'approccio al fenomeno è basato in modo particolare sulla difesa della privacy. Per questo, almeno a livello di dichiarazioni di principio, la soluzione del consenso preventivo (opt-in) viene ritenuta migliore di quella opt-out (in cui un messaggio propositivo è permesso). L'interpretazione della legge si scontra con due problemi. Il primo è che non è dato per scontato che l'indirizzo e-mail sia veramente un dato personale: esso infatti non identifica necessariamente un individuo in modo univoco. In Italia la situazione è stata definita con una certa chiarezza, ma alcuni osservatori<sup>3</sup> hanno ancora dei dubbi. Inoltre, e questo è il secondo problema, la legge sulla privacy è applicabile solo se il dato personale non è stato pubblicato in elenchi o registri pubblici. Anche in questo caso, l'Italia ha provveduto a stabilire che i gruppi di discussione, i forum elettronici o le pagine web non sono equiparabili a elenchi pubblici, quindi i dati lì pubblicati sono ancora tutelati dalla legge sulla privacy. In Europa, poi, si presta particolare attenzione al lato commerciale dello spamming: il principio è che il costo della pubblicità deve essere sopportato da chi la fa e non da chi la subisce. Ma in questo modo tutto lo spamming che non è commerciale sfugge alla regolamentazione legale.

Negli Stati Uniti d'America, invece, le leggi in vigore in alcuni Stati tentano soprattutto di impedire lo sfruttamento di risorse di terzi senza l'accordo dei legittimi proprietari. Non mancano però coloro che vorrebbero regolamentare la posta elettronica sulla base del contenuto. Questo errore deriva dal considerare lo spamming come un'espressione esclusivamente commerciale. Una legge che stabilisce che un messaggio è legale e un altro non lo è in base al contenuto può essere in contrasto con gli articoli costituzionali sulla libertà d'espressione (negli USA ma anche in Europa) e, personalmente, la riterrei pericolosamente vicina alla censura.

---

<sup>3</sup> **Andrea Monti**, *Spam e indirizzi e-mail. Quando la 675 è impotente*, 15 febbraio 2001, in InterLex, <http://www.interlex.it/675/amonti44.htm> (consultato il 18 novembre 2002).

### 6.4.1. In Italia

Grazie alla legislazione italiana sulla privacy una vittima di spamming ha potuto ottenere una significativa vittoria legale, ottenendo un risarcimento per il danno subito. La base legale risiede nella legge sulla «Tutela delle persone rispetto al trattamento dei dati personali» (675/96<sup>4</sup>). Il Garante per la protezione dei dati personali ha sancito che l'indirizzo di posta elettronica rientra tra i dati personali (l'esempio è riportato tra breve). Il Garante ha anche stabilito che, senza preventivo ed esplicito consenso, è illegittimo utilizzare indirizzi di posta elettronica prelevati da gruppi di discussione, forum, pagine web e simili, in quanto questi non sono parte degli elenchi pubblici<sup>5</sup> e quindi non rientrano nelle eccezioni previste dalla legge 675/96.

Il decreto legge 171 (13 maggio 1998) stabilisce che «l'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del telefax per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato.»<sup>6</sup> Lo spamming via e-mail è certamente un sistema automatizzato. Il principio alla base di questo decreto è che i costi pubblicitari devono essere interamente sostenuti da chi effettua una comunicazione pubblicitaria, e non da chi la subisce. L'oggetto della comunicazione dev'essere di tipo commerciale, obbligando l'azienda a chiedere un consenso preventivo (opt-in), ma escludendo dall'applicazione tutti i messaggi di spam politici, religiosi o altro. Un altro decreto, il DL 185 del 22 maggio 1999, stabilisce che «l'impiego da parte di un fornitore del telefono, della posta elettronica di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore.»<sup>7</sup> In questo decreto ci si riferisce esplicitamente alla posta elettronica.

L'esempio a cui accennavo riguarda un ricorso inoltrato da una vittima di spamming. Vorrei esporre il procedimento come descritto dal protagonista, Massimo Cavazzini<sup>8</sup>. Un ricorso di questo tipo è applicabile allo spam che proviene dall'Italia o riguarda aziende italiane. In Italia infatti la citata legge sulla privacy è molto forte, ma gli altri Paesi europei hanno leggi più o meno simili perché tutte derivano dalla stessa direttiva comunitaria. Il primo passo intrapreso dalla vittima in questione è stato quello di richiedere alcune informazioni allo spammer: la legge 675/96 dà il diritto di conoscere in tempi brevi chi è il titolare del trattamento dei propri dati

---

<sup>4</sup> *Tutela dei dati personali - Legge 675/96*, <http://www.interlex.it/675/indice.htm> (consultato il 18 novembre 2002).

<sup>5</sup> *Decisione dell'11 gennaio 2001, Raccolta e trattamento di caselle di posta elettronica attraverso procedure di spamming per comunicazioni politiche*, <http://www.interlex.it/testi/d010111.htm> (consultato il 19 novembre 2002).

<sup>6</sup> *Decreto legislativo 13 maggio 1998, n. 171*, <http://www.interlex.it/testi/dlg98171.htm> (consultato il 18 novembre 2002).

<sup>7</sup> *Decreto legislativo 22 maggio 1999, n. 185*, <http://www.interlex.it/testi/dlg99185.htm> (consultato il 18 novembre 2002).

<sup>8</sup> **Massimo Cavazzini**, *Combattere lo spam, come colpire gli spammer al portafogli*, <http://www.maxkava.com/spam/> (consultato il 14 novembre 2002).

personali, quali sono le finalità di tale trattamento e quali le sue modalità, da dove vengono i dati (anche nel caso siano stati acquistati da società terze) e quando è stato autorizzato il loro trattamento. Avendo ricevuto risposta negativa, è stato presentato il ricorso al Garante. Nel caso descritto, Massimo Cavazzini ha ottenuto una piena informazione sui suoi dati e la loro rimozione dalle banche dati dell'azienda, nonché un risarcimento di 250 € perché la sua privacy era stata violata. Non è una cifra notevole, ma vista la quantità di messaggi di spam normalmente inviata, se molti destinatari inoltrassero un tale ricorso, per lo spammer la somma potrebbe diventare rapidamente molto importante. Colpire gli spammer al portafogli potrebbe essere uno dei modi migliori per combattere lo spamming. Le leggi italiane danno questa possibilità concedendo al destinatario il diritto di rimuovere la propria iscrizione (opt-out), ma non garantiscono in modo assoluto l'obbligo del consenso preventivo (opt-in).

#### **6.4.2. Nell'Unione Europea**

La situazione italiana rispecchia quella europea. Anche nell'Unione Europea la lotta allo spamming ha come strumento la legislazione per la tutela dei dati personali

Sembra che l'UE abbia preso coscienza del problema: recentemente è stata approvata una nuova direttiva (la 2002/58/CE<sup>9</sup>) che segna una svolta nel settore della tutela dei dati personali. L'articolo 13 disciplina lo spamming, ma solo quello riguardante la commercializzazione diretta. Al contrario di quanto accade nella definizione di spamming data, si tiene conto del contenuto del messaggio escludendo dalla regolamentazione le comunicazioni riguardanti sia il commercio tra aziende sia i messaggi di tipo politico, elettorale, religioso, d'intrattenimento o altro. Ma il punto importante è che viene sancito il principio dell'opt-in: le aziende che desiderano fare pubblicità automatica via e-mail dovranno avere il consenso preventivo dei destinatari. Tutte le comunicazioni non automatiche non rientrano nella sfera di quelle sottoposte a opt-in. L'Unione Europea intende però tutelare in qualche modo i destinatari proibendo esplicitamente la modifica dei dati del mittente celando l'identità o evitando di fornire un indirizzo valido a cui inviare una richiesta per far cessare l'invio dei messaggi.

#### **6.4.3. In Svizzera**

La situazione svizzera è molto simile a quella italiana ed europea: la base legale per combattere lo spamming si trova nella Legge federale sulla protezione dei dati (LPD<sup>10</sup>) del

---

<sup>9</sup> *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, [http://www.interlex.it/testi/02\\_58ce.htm](http://www.interlex.it/testi/02_58ce.htm) (consultato il 19 novembre 2002).

<sup>10</sup> *Legge Federale del 19 giugno 1992 sulla protezione dei dati (LPD)*, [http://www.admin.ch/ch/i/rs/c235\\_1.html](http://www.admin.ch/ch/i/rs/c235_1.html) (consultato il 19 novembre 2002).

1992. In particolare, la legge vieta di trattare i dati personali senza l'autorizzazione dell'interessato, ma permette l'uso di tali dati se essi sono pubblici e l'interessato non si è esplicitamente opposto al trattamento. Quindi, il diritto alla disiscrizione (opt-out) è garantito, ma di principio lo spamming non è vietato.

I problemi nell'interpretazione della legge sono simili a quelli accennati per l'Italia e per l'Unione Europea. L'indirizzo di posta elettronica rientra tra i dati qualificati come personali? I forum elettronici, i gruppi di discussione, le directory sono elenchi pubblici?

Queste sono solo alcune delle domande fondamentali a cui giuristi ed esperti di Internet stanno cercando di dare una risposta.

#### **6.4.4. Negli USA e in Giappone**

Negli Stati Uniti d'America, a livello federale, vi è qualche discussa proposta di legge anti-spam, ma finora nessuna è stata approvata. A livello statale, invece, molti governi si sono mossi. Il problema in questo caso è quello della giurisdizione: le leggi statali sono applicabili solo se il mittente o le strutture interessate sono nello Stato in questione. Nonostante questa limitazione in alcuni casi è stato possibile punire spammer con multe fino a svariate migliaia di dollari.

Il primo Stato a introdurre una legislazione anti-spam è stato il Nevada nel 1997. Le leggi statali vietano, nella maggior parte dei casi, l'invio di messaggi e-mail non sollecitati usando un dominio di un terzo senza permesso, oppure camuffando il punto d'origine o le informazioni di routing. È illegale anche distribuire software per questi scopi. In alcuni degli Stati dell'Unione chi desidera inviare messaggi commerciali di massa non sollecitati deve indicare le istruzioni per rimuovere l'iscrizione e un indirizzo valido per farlo. La massa viene quantificata in alcuni casi in più di 500 destinatari, in altri si parla di più di mille. Ogni contenuto erotico esplicito è vietato, ma non è proibito pubblicizzare prodotti a luci rosse se indicato chiaramente nel soggetto del messaggio. Alcuni Stati prevedono l'uso di una sigla nel soggetto che identifichi tutte le comunicazioni di questo tipo (la sigla è "ADV", per "advertisement"). In caso di abusi, il provider ha il diritto di intervenire chiudendo l'acconto dello spammer.

In Giappone, invece, sono in vigore alcune normative che puniscono duramente chi invia messaggi promozionali ai destinatari che hanno esplicitamente chiesto di non riceverli. Si tratta di un procedimento a opt-out fortemente voluto dal mondo economico e che riguarda sia la posta elettronica che la telefonia mobile.

## 7. Contromisure tecniche

La tecnologia, senza la quale lo spamming non esisterebbe, ci dà anche qualche strumento per evitarlo e contrastarlo. Le proposte di soluzioni tecniche che ho trovato in Rete hanno come scopo il contenimento dell'invio o della ricezione di spamming. Oltre ad alcune tecniche per non finire negli indirizzi degli spammer, mascherando il proprio indirizzo, esistono dei software per filtrare i messaggi indesiderati a livello client (per l'utente) e server (per l'amministratore di server e-mail).

In questo ambito, i primi a muoversi sono stati gli utenti più smaliziati, che hanno tentato di arginare il fenomeno dello spamming localmente con alcuni artifici. Poi gli amministratori dei server di posta elettronica e i provider hanno iniziato a prendere in seria considerazione l'ipotesi di intervenire tecnicamente per limitare lo spamming. Infine sono arrivate le aziende di software che hanno iniziato a rilasciare prodotti per utenti finali e per provider.

Gli utenti hanno anche tentato di agire in modo comunitario: ancora oggi sono numerose le organizzazioni che incitano alla rivolta, a volte con successo. Molti provider si sono attrezzati per combattere gli abusi dopo aver subito pressioni da parte di utenti, sia loro clienti che estranei. Gli spammer stessi, avendo ricevuto proteste via Internet e nel mondo reale, hanno adottato alcune tecniche per mascherare la provenienza dei messaggi e usare domini falsi, permettendo, in alcuni casi, di riconoscerli più facilmente. Le proteste hanno tenuto lontano dallo spamming molte grosse aziende, impaurite dagli effetti negativi sulla loro immagine. La rivolta è ancora più efficace se messa in atto dai clienti: le aziende che pubblicizzano i loro prodotti vengono incentivate a indicare chiaramente scopi e modalità della raccolta di indirizzi e ad aderire a servizi come TRUSTe. A volte però le cose sono degenerare in attacchi di tipo mail-bombing o denial-of-service, anche contro innocenti.

Oggi abbiamo a disposizione una grande quantità di risorse tecniche per evitare di ricevere spam, grazie anche alle numerose organizzazioni che si occupano di informare i navigatori. Ma quanto sono realmente efficaci questi strumenti? E quali gli svantaggi e i problemi che possono causare? Ho cercato di rispondere a queste domande.

Dal punto di vista tecnico, si possono identificare alcune caratteristiche che si ritrovano in diversi strumenti. Alcuni di essi utilizzano delle parole chiave per identificare i messaggi di spam. Le parole chiave possono essere cercate nel corpo del messaggio o, più frequentemente, nell'header. In questo caso vengono analizzati soprattutto il campo From, alla ricerca dei mittenti noti di spam, e il campo Subject, dove gli spammer tendono a usare espressioni simili.

Vengono anche cercate irregolarità di protocollo che dovrebbero essere assenti dai messaggi partiti da server configurati correttamente. I sistemi più raffinati usano metodi statistici e analizzano le parole di tutto il messaggio per decidere se si tratta di spam o no. L'intervento dell'utente è limitato a indicare al software i messaggi di spam che sono sfuggiti ai filtri.

Esistono degli strumenti il cui funzionamento dipende largamente dal feedback dato da parte degli utenti, in vari modi. Si creano così delle reti collaborative grazie alle quali un utente può segnalare ai gestori del servizio i messaggi di spam ricevuti, i quali poi aggiornano automaticamente gli altri utenti attraverso il software. Questa collaborazione funziona sia per i tool gratuiti che per quelli commerciali. In quest'ultimo caso, è l'azienda produttrice a sfruttare le strutture dei clienti per osservare lo spam in circolazione ed adeguare quotidianamente i filtri. Alcune aziende fanno anche uso di indirizzi trappola, sparsi per la rete con lo scopo di ricevere messaggi di spam che verranno analizzati.

Lo scopo del feedback è quello di creare strumenti in grado di imparare dall'esperienza e di tenersi aggiornati sulle pratiche usate dagli spammer.

## 7.1. Organizzazioni

Vi sono moltissime organizzazioni e gruppi più o meno amatoriali attivi nella lotta contro lo spamming. Alcuni di essi offrono veri e propri strumenti, mentre altri sono semplicemente siti a carattere informativo.

Uno dei punti di riferimento più noti è [spam.abuse.net](http://spam.abuse.net/)<sup>1</sup>, che si definisce la miglior raccolta di link anti-spam. Tra i documenti si trovano alcune guide di rapida consultazione e informazioni mirate agli utenti, agli amministratori di sistema e a chi intende occuparsi di e-mail marketing. [Fighters4web](http://www.fighters4web.com/)<sup>2</sup> ne ha tradotto quasi tutti i documenti in italiano diventando il mirror ufficiale per l'Italia. Inoltre, come associazione di volontari, si propone come intermediario tra gli utenti e i responsabili degli uffici reclami di alcuni provider italiani.

Legata a [spam.abuse.net](http://spam.abuse.net/) (il presidente è sempre Scott Hazen Mueller) troviamo la CAUCE (Coalition Against Unsolicited Commercial Email) e la consociata europea EuroCAUCE<sup>3</sup>. CAUCE e le sue consociate nazionali sono attive soprattutto quando si tratta di informare soggetti istituzionali a proposito di proposte di legge.

---

<sup>1</sup> **spam.abuse.net**, <http://spam.abuse.net/>.

<sup>2</sup> **Fighters4web**, <http://www.fighters4web.com/>.

<sup>3</sup> **CAUCE**, <http://www.cauce.org/> e **EuroCAUCE**, <http://www.euro.cauce.org/>.

Negli USA esiste anche la fondazione SpamCon<sup>4</sup> che, in modo simile a spam.abuse.net, offre informazioni per gli utenti, gli amministratori di sistema e gli esperti di marketing interessati all'e-mail, oltre a un'intera sezione dedicata alla legge. Tra i link disponibili, vi sono anche i riferimenti ad alcune aziende che offrono mailbox filtrate. SpamCon offre direttamente un servizio di indirizzi DEA (disposable email address), cioè indirizzi che possono avere una durata limitata, dopo la quale vengono cancellati. Sono utili se si manda qualche messaggio in un forum pubblico o si ha necessità di riempire un form su un sito web del quale non ci si fida del tutto.

Due preziosi centri di informazione sono spamfaq.net<sup>5</sup> e Petemoss.com<sup>6</sup>. Il primo raccoglie tutte le domande frequenti (FAQ) del gruppo di discussione Usenet *news.admin.net-abuse.e-mail*, mentre il secondo fornisce una ventina di notizie al giorno che hanno lo spamming come tema. Esistono poi alcuni archivi di messaggi di spam, come per esempio Spam Archive<sup>7</sup> o lo Spam Recycling Center<sup>8</sup>, che hanno entrambi la finalità di raccogliere i messaggi di spam ricevuti da chiunque, in Rete, e di fornirli come archivi per i test su software anti-spam o per ricerche di altro genere. Si trovano anche numerosi archivi privati ed è disponibile il gruppo di discussione su Usenet *news.admin.net-abuse.sightings*.

In Italia è nato circa un anno fa il sito NoSpamWare<sup>9</sup>, ma da qualche tempo non viene più aggiornato. Vi si possono trovare molte informazioni in italiano. Una delle prime guide italiane sullo spamming è sicuramente quella di Leonardo Collinelli<sup>10</sup> che viene aggiornata periodicamente. Si tratta di un vero e proprio manuale completo e preciso. In Svizzera, invece, il sito di riferimento è spam.trash.net<sup>11</sup>, in tedesco, mentre la mailing list spam-ch<sup>12</sup> è un punto d'incontro tra persone competenti. Uno degli argomenti più discussi è lo spamming di Martin Fürst, un personaggio che più volte è stato colto in fallo ma che sembra impossibile fermare.

---

<sup>4</sup> **SpamCon Foundation**, <http://www.spamcon.org/>.

<sup>5</sup> **spamfaq.net**, <http://www.spamfaq.net/>.

<sup>6</sup> **Petemoss.com**, <http://www.petemoss.com/>.

<sup>7</sup> **Spam Archive**, <http://www.spamarchive.org/>.

<sup>8</sup> **Spam Recycling Center**, <http://www.spamrecycle.com/>.

<sup>9</sup> **NoSpamWare**, <http://www.nospamware.it/>.

<sup>10</sup> **Pagina Antispam in italiano**, <http://www.collinelli.net/antispam/>.

<sup>11</sup> **Information zum Thema Spam**, <http://spam.trash.net/>.

<sup>12</sup> **spam-ch**, <http://www.verboten.net/mailman/listinfo/spam-ch>.

## 7.2. Strumenti per l'utente

Chi naviga in Internet e usa la posta elettronica può ricorrere ad alcune soluzioni per difendersi dal dilagare dello spamming, soluzioni che hanno una validità limitata perché agiscono a livello di ogni singolo utente e non affrontano il problema nella sua globalità. Gli spammer sanno che i loro messaggi non vengono letti (chi li riceve li guarda il tempo necessario per cestinarli), ma questo non li scoraggia perché sono interessati al guadagno. Sembra quindi che non saranno scoraggiati nemmeno dall'idea che ogni utente filtri in modo automatico tali messaggi.

Comunque, per iniziare, vale la pena ricordare due raccomandazioni tipiche. La prima è quello di non rispondere assolutamente ai messaggi si spam, nemmeno se viene riportata l'assicurazione che se si risponde dicendo di rimuovere il proprio indirizzo dalla lista di destinatari si verrà accontentati. Infatti sono troppi gli spammer che abusano di questo tipo di diciture al fine di ricevere una conferma della validità dell'indirizzo. Chi desidera fare e-mail marketing dovrà trovare altre strade per garantire la possibilità di opt-out.

La seconda raccomandazione è quella di non acquistare i prodotti venduti tramite spam, di non seguire i link e non visitare i siti indicati. Vi sono poi alcune tecniche che l'utente può mettere in pratica.

### 7.2.1. Tecniche per i forum

Chi scrive regolarmente in qualche forum pubblico o in un gruppo di discussione può utilizzare l'artificio di modificare l'indirizzo nel campo From in modo che un programma automatico lo scambi per un indirizzo reale. L'efficacia di tale metodo è abbastanza dubbia e, se qualcuno vuole rispondere legittimamente all'indirizzo di posta elettronica e non pubblicamente sul forum, deve essere in grado di risalire al vero indirizzo. Ricordo che, per quanto riguarda Usenet, tale metodo è in contrasto con quanto indicato dalla RFC 1036<sup>13</sup>: in essa si raccomanda fortemente (quindi è obbligatorio a meno di ragioni particolarmente gravi) che il campo From di un messaggio Usenet sia l'indirizzo valido del mittente. Impedire una funzione della Rete per fermarne un'altra non è la risposta.

Per fare un esempio di questo tipo di artificio, il mio indirizzo (*mfare@swissonline.ch*) potrebbe diventare *mfareXXX@swissonline.ch*, *mfare@XXX.swissonline.ch* oppure *mfare@swissonline.XXX.ch*, dove XXX è una stringa scelta dall'utente stesso.

---

<sup>13</sup> M. Horton, RFC-1036: Standard for Interchange of USENET Messages, dicembre 1987, <http://www.ietf.org/rfc/rfc1036.txt> (consultato il 15 settembre 2002).

Per questo tipo di modifica bisogna fare attenzione al contenuto della stringa aggiunta e alla sua posizione. Al posto di XXX si può usare qualsiasi cosa: nospam, toglimi, rimuovimi, eccetera. Dev'essere però qualcosa che un essere umano sia in grado di riconoscere e di eliminare se desidera rispondere. Inutile dire che, come dimostrato nel capitolo 5.2.1., è molto semplice per uno spammer rimuovere tali stringhe, se ne ha voglia.

Comunque, se si desidera usare questa tecnica, bisogna scegliere con cura la posizione della stringa. Nel primo caso (*mfareXXX@swissonline.ch*) l'inconveniente è causato dallo spammer che usa l'indirizzo così com'è. Il suo messaggio di spam arriverà al server di posta giusto, ma non potrà essere recapitato perché l'utente non esiste. Quindi, il server di posta avrà ugualmente del lavoro da compiere (ricerca dell'utente, generazione del messaggio d'errore). Inoltre alcuni server sono configurati in modo da mandare a un amministratore tutti i messaggi per i quali l'utente specificato non è valido. Il secondo caso (*mfare@XXX.swissonline.ch*) sembra essere il migliore, anche se comunque i server DNS devono svolgere del lavoro ed eventualmente potrebbe essere coinvolto anche un server di posta. Nell'ultimo caso (*mfare@swissonline.XXX.ch*), il dominio apparente di provenienza è *XXX.ch*, dominio che, presumibilmente, non è valido. Il rischio è che alcuni mail o news server rifiutino il messaggio proprio perché sembra provenire da un dominio inesistente.

Da un punto di vista comunicativo questo tipo di alterazioni sono un ostacolo per una comunicazione scorrevole e rischiano di avere più controindicazioni che benefici: molti utenti non sono pratici e non rimuovono l'alterazione. Dopo aver risposto ricevono un messaggio d'errore che spesso non capiscono e non ritentano. Per provare questo metodo ho inviato a quattordici conoscenti (alcuni navigatori esperti, altri meno) un messaggio chiedendo di mandarmi una risposta. Ho alterato il campo From, mettendo *mfare@swissonline.toglimi.ch*, e in fondo al messaggio ho inserito le istruzioni per replicare. Intendevo dimostrare che usare un indirizzo contraffatto contro lo spam non serve e può essere dannoso perché chi desidera replicare incontra difficoltà.

Nessuno di quelli che hanno ricevuto il messaggio ha risposto facilmente: solo due persone sono riuscite a rispondere, ma dopo aver compiuto alcuni tentativi; quattro persone non ci sono riuscite e otto persone non l'hanno ricevuto. Pur non essendo un test rappresentativo, è indicativo perché effettivamente la comunicazione è stata intralciata.

Però, questa tecnica può effettivamente evitare lo spam: ho inviato al gruppo di discussione *alt.alcohol* due messaggi, usando come mittenti *ml09@ml.ti-edu.toglimi.ch* e *mlc09@cherou.toglimi.com*. Queste sono alterazioni di due indirizzi che TI-EDU mi ha messo a disposizione e che non ho usato per altri scopi. I due messaggi sono stati inviati il 21 ottobre

2002 e si sono propagati su diversi news server (infatti sono consultabili su GoogleGroups), ma al 7 gennaio 2003 le due caselle erano ancora completamente vuote.

Nonostante la probabile efficacia di questo sistema, credo che non sia una soluzione valida proprio a causa degli impedimenti causati alla normale comunicazione. Inoltre non sono molte le persone che scrivono nei gruppi di discussione, ma lo spamming è un problema per tutti gli utenti Internet.

### 7.2.2. Tecniche per le pagine web

Per quanto riguarda invece la pubblicazione di indirizzi su pagine web, esistono alcuni metodi per rendere le cose difficili a chi è in cerca di indirizzi per spamming. Per esempio, gli indirizzi possono essere scritti come testo, ma non come riferimento (cioè senza un tag `<A mailto:"user@domain.tld"> user@domain.tld </A>`), sostituendo la chiocciola con una parola (per esempio "user at domain tld"). Oppure si può usare un'immagine nella quale è riportato l'indirizzo. Però questi metodi hanno lo stesso problema di quello di cui si è detto poco sopra: rischiano di intralciare la comunicazione. Un metodo semplice e completamente trasparente per l'utente finale è quello di usare qualche riga di javascript per stampare a video l'indirizzo senza che questo sia effettivamente contenuto nel codice HTML.

Uno script può essere quello che segue, realizzato presso l'USI da Jacopo Armani:

```
<script language="JavaScript">

<!--
/* Print Email, v1.0                                     */
/* ANTI-SPAM                                           */
/* Hide email address to spiders                       */
/* Author: Jacopo Armani (pako@ngi.it)                */
var def_domain = "yourdomain.com";
var URL = window.location.href;

function printEmail(user, domain) {
    // if domainName has been passed, we use it
    if (domain == null) {
        domain = def_domain;
    }

    // creates the email string
    var email;
    email = user;
    email = email + "@";
    email = email + domain;
    document.write ("<a href='mailto:" + email + "'> " +
email + "</a>");
}
//-->

</script>
```

La chiamata alla funzione avviene come segue:

```
<script language="JAVASCRIPT">
  <!--
  printEmail("mfare", "swissonline.ch")
  //-->
</script>
```

In questo modo l'indirizzo non appare mai per intero nel codice HTML, ma viene stampato sul video e funziona come riferimento cliccabile. I programmi automatici non saranno in grado di rilevarlo, fino a quando non integreranno un interprete javascript.

Anche in questo caso ho fatto un piccolo test: il 10 giugno del 2002 è stata pubblicata una pagina web presso il sito di TI-EDU (l'indirizzo preciso è <http://www.ti-edu.ch/servizi/informatica/tesi-fare.html>). La pagina è collegata tramite un link nascosto alla pagina iniziale del sito e riporta quattro indirizzi: *ml10@ml.ti-edu.ch*, *mlc10@cherou.com*, *ml11@ml.ti-edu.ch*, *mlc11@cherou.com*. I primi due sono stati pubblicati in chiaro, i secondi due con lo script di Jacopo Armani. Il 7 gennaio 2003 i messaggi di spam giunti sugli indirizzi arrivati in chiaro erano uno per *ml10@ml.ti-edu.ch* e otto per *mlc10@cherou.com*. Sugli indirizzi protetti dallo script non è arrivato nulla. Si veda il capitolo 8 per ulteriori approfondimenti.

### 7.2.3. Filtri e software: alcuni esempi

Un altro modo che l'utente ha a disposizione per evitare di ricevere spam è il ricorso a filtri a livello di client, vale a dire filtri che agiscono sul PC dell'utente.

I filtri sul client non obbligano a cancellare automaticamente i messaggi che rilevano come spam: di solito permettono di deviarli in un'apposita cartella che si controlla ogni tanto. Lo scopo di questi filtri è quello di non perdere tempo a cancellare i messaggi di spam. Quasi ogni tipo di filtro è configurabile in base ai campi del messaggio e agisce in base a stringhe di testo tipiche dei messaggi di spam, che non appaiono nei messaggi regolari. Si possono per esempio filtrare i messaggi che non contengono nel campo To l'indirizzo effettivo del destinatario oppure il cui soggetto sia tutto in maiuscolo. Un altro criterio si rifà al campo From: se esso è vuoto, o il mittente risponde a certe caratteristiche, il messaggio viene filtrato. Questi sistemi non sono molto efficaci perché si possono aggirare facilmente. Alcuni di essi sono un po' più evoluti e possono essere configurati per rifiutare la posta proveniente da domini che non esistono, tramite un controllo. È un sistema efficace, ma gli spammer possono usare domini e indirizzi reali. Un metodo diffuso è quello di rifiutare i messaggi provenienti da server elencati

in una lista nera (blacklist) oppure accettare solo quella proveniente da una lista di autorizzati (whitelist). Quest'ultimo approccio è estremo e senz'altro efficace, ma impedisce di ricevere messaggi da sconosciuti e ha molti inconvenienti. Le blacklist invece raccolgono gli indirizzi o i domini da cui si è ricevuto qualche messaggio di spam. In realtà, gli spammer cambiano indirizzo praticamente a ogni invio, inoltre spesso non è possibile filtrare un intero dominio esistente perché da esso scrivono altri utenti legittimati a farlo. L'efficacia di questo tipo di blacklist è quindi dubbia. Un discorso diverso va fatto per le blacklist utilizzate dagli amministratori di server e-mail, di cui parlerò più avanti.

Inizialmente si usavano tool molto semplici di cui il killfile è il migliore esempio. È una lista di indirizzi da cui non si desidera ricevere messaggi. Esso è nato per nascondere i messaggi dei provocatori (troll), ma è applicabile anche allo spam perché è molto flessibile. Il killfile poi si è evoluto e per i sistemi Unix oggi sono a disposizione file di configurazione molto complessi per software come procmail (un programma che processa i messaggi quando questi arrivano nella casella locale). Uno di questi, SpamBouncer<sup>14</sup>, è in grado di generare dei falsi messaggi di errore per far credere allo spammer che l'indirizzo è inesistente.

Vorrei proporre alcuni esempi di software e tool anti-spam disponibili per l'utente medio. Uno di questi viene dall'Italia e si chiama Spam Terminator<sup>15</sup>. Il programma, gratuito e disponibile solo per Windows, si situa tra il client di posta e il server POP3. Il client viene configurato per usare Terminator come server, mentre Terminator accede al server reale e, prima di scaricare la posta, ripulisce la mailbox da eventuali messaggi di spam. I criteri, personalizzabili, sono contenuti in una lista che si può aggiornare dal sito di Spam Terminator. Anche SpamPal<sup>16</sup> funziona nello stesso modo, ma è lui stesso a cercare gli aggiornamenti automaticamente. SpamEater<sup>17</sup>, invece, è un po' diverso: dopo essere stato configurato, si collega periodicamente (in modo automatico o manuale) al server POP e ripulisce la mailbox. I messaggi di spam rilevati possono essere salvati in un apposito spazio o eliminati. È interessante notare che SpamEater è integrato con SpamCop (che verrà approfondito nel capitolo 7.2.6.) e quindi è possibile mandare automaticamente i reclami. I criteri adottati per i filtri non sono molto diversi rispetto a quelli dei software visti finora. SpamKiller<sup>18</sup> è il nome del prodotto di McAfee che blocca i messaggi di spam con liste costruite dalle trappole di McAfee, aggiorna i filtri automaticamente, è utilizzabili con molteplici protocolli (POP3, MAPI e Hotmail), crea

---

<sup>14</sup> **SpamBouncer**, <http://www.spambouncer.org/> .

<sup>15</sup> **Spam Terminator**, <http://www.sertel.net/terminator/> .

<sup>16</sup> **SpamPal**, <http://www.spampal.org.uk/> .

<sup>17</sup> **SpamEater**, <http://www.hms.com/spameater.asp> .

<sup>18</sup> **SpamKiller**, <http://www.mcafee.com/myapps/msk/default.asp> .

una lista di “amici” automaticamente, permette la gestione di più account di posta, confeziona reclami per ogni spam.

Una soluzione interessante è quella proposta da SpamAssassin<sup>19</sup>. Si tratta di un software che identifica lo spam. Pur essendo pensato per sistemi Unix, grazie al fatto di essere open source esso esiste anche come add-in per alcuni programmi commerciali<sup>20</sup>. Per identificare lo spam vengono effettuati una serie di test sull’header e sull’analisi del testo del messaggio. Inoltre vengono usate alcune blacklist reperibili in Rete. Dopo essere stato identificato, lo spam viene marchiato con un punteggio per essere filtrato dal programma di posta abituale. SpamAssassin usa anche Vipul’s Razor<sup>21</sup>, una rete distribuita e collaborativa di identificazione dello spam che opera da un paio d’anni, grazie alla quale è stato costruito un catalogo costantemente aggiornato dello spam in propagazione. Grazie a questo catalogo, SpamAssassin (ma anche altri software) possono verificare facilmente se un messaggio è spam o no. Vipul’s Razor è una rete che ha come attori principali gli utenti, quasi come nel peer-to-peer di Napster o simili, e che vive grazie alla comunità di Internet. L’evoluzione commerciale di Vipul’s Razor si chiama SpamNet ed è gestita da Cloudmark<sup>22</sup>.

Se non ci si vuole cimentare nell’installazione e nella configurazione di filtri sul proprio computer, è possibile far capo a servizi esterni. Il funzionamento è molto semplice: il proprio indirizzo e-mail lo si tiene segreto e si comunica pubblicamente solo quello del servizio anti-spam scelto. Tutta la posta arriva quindi all’indirizzo anti-spam, viene esaminata e solo quella che supera l’esame verrà inoltrata al proprio indirizzo reale. Questo servizio è disponibile sia gratuitamente (per esempio, presso Despammed<sup>23</sup>) che a pagamento (Spamex<sup>24</sup> lo offre per 9.95 dollari all’anno).

L’ultimo prodotto che presento è Spam Arrest<sup>25</sup>: per 20 dollari ogni sei mesi è possibile proteggere la propria mailbox con uno stratagemma. Il software è basato su una whitelist, una lista di amici autorizzati a scriverci. Se qualcuno che non è nella lista scrive a una mailbox protetta da Spam Arrest, riceverà immediatamente un messaggio che lo invita a visitare un sito, da cui può iscriversi alla lista di amici. Per poterlo fare, dovrà trascrivere in un campo testo di

---

<sup>19</sup> **SpamAssassin**, <http://eu.spamassassin.org/> .

<sup>20</sup> Per Outlook: <http://www.deersoft.com/e> per Eudora: <http://www.spamnix.com/>. Nel gennaio 2002 Deersoft è stata acquistata da Network Associates Inc. e pare che verrà rilasciato un nuovo prodotto marchiato McAfee entro 6 mesi.

<sup>21</sup> **Vipul’s Razor**, <http://razor.sourceforge.net/> .

<sup>22</sup> **Cloudmark**, <http://www.cloudmark.com/> .

<sup>23</sup> **Despammed**, <http://www.despammed.com/> .

<sup>24</sup> **Spamex**, <http://www.spamex.com/> .

<sup>25</sup> **Spam Arrest**, <http://www.spamarrest.com/> .

un form una parola mostrata come immagine. In questo modo non è possibile iscriversi automaticamente. Dopo questa iscrizione, tutti gli altri messaggi viaggeranno normalmente.

#### 7.2.4. Reverse Spam Filtering

Vorrei esporre due soluzioni che si distinguono per la loro originalità. La prima è stata ideata da un'esperta utente di Internet<sup>26</sup>. La sua strategia non è quella di cercare lo spam, ma di selezionare ciò che non è spam e mandare tutto il resto in una mailbox speciale, che viene controllata solo periodicamente. I messaggi vengono esaminati tramite una serie di test binari (sì/no) e distribuiti in diverse mailbox. Dapprima il sistema controlla se il messaggio in entrata appartiene a qualche invio di massa sollecitato (mailing list o newsletter). In questo caso viene messo nella mailbox dedicata alle mailing list e alle newsletter. Nel caso in cui la risposta sia negativa, viene controllata la provenienza: se viene da indirizzi approvati (cioè definiti in una lista di "amici") viene posto nella mailbox degli amici, altrimenti il messaggio viene analizzato e quindi marchiato come spam secondo un livello di probabilità. In seguito viene inserito nella speciale mailbox per i messaggi sospettati di essere spam, il cui contenuto può essere ordinato in base al punteggio di probabilità di spam assegnato e quindi manualmente controllato per cercare eventuali messaggi che non sono spam ma che sono finiti lì per errore.

Questa soluzione necessita di un buon software per filtrare i messaggi, uno per analizzare e assegnare un punteggio di probabilità ai messaggi sospettati di essere spam, un buon client di posta che permetta di gestire più mailbox e di ordinare il contenuto delle mailbox in base a criteri personalizzati, un sistema per mantenere facilmente o automaticamente una lista di indirizzi "amici" aggiornata. L'autrice usa Procmal per filtrare i messaggi in arrivo, SpamAssassin per marciare i messaggi con un punteggio di spam, Mulberry e Pine per controllare e gestire la posta in arrivo, uno script artigianale che mantenga la lista di "amici" prendendoli dai messaggi in uscita e dal suo indirizzario privato.

#### 7.2.5. Filtri bayesiani

La soluzione di Paul Graham<sup>27</sup>, in fase di sviluppo teorico, è basata su uno studio statistico del contenuto dei messaggi e interessa chi si occupa di software anti-spam. Nonostante la definizione di spamming non tenga conto del contenuto dei messaggi, Graham sostiene che il destinatario umano usa proprio il contenuto per riconoscere i messaggi di spam. Per

---

<sup>26</sup> Nancy McGough, *Reverse spam filtering - Winning Without Fighting*, 4 settembre 2002, in Infinite Ink, <http://www.ii.com/internet/messaging/spam/> (consultato il 2 dicembre 2002).

<sup>27</sup> Paul Graham, *A plan for spam*, agosto 2002, <http://www.paulgraham.com/spam.html> (consultato il 2 dicembre 2002).

automatizzare questo algoritmo, Graham propone l'utilizzo di un filtro bayesiano che combina le probabilità della presenza di singole parole nel messaggio di spam. L'algoritmo anti-spam bayesiano decide in base alle parole contenute nei messaggi se un messaggio è spam o no.

Prima di illustrare l'algoritmo espongo un esempio per spiegare il teorema di Bayes: abbiamo un'osservazione O ("una moneta è stata lanciata 6 volte con 4 teste") e un'ipotesi H ("la moneta non è truccata"). Sappiamo come calcolare  $P(O|H)$ , cioè la probabilità che O accada dato H, cioè la probabilità che escano 4 teste su 6 lanci, sapendo con che probabilità la moneta è onesta. Ci interessa però sapere  $P(H|O)$ , cioè la probabilità che H accada, dato O, e cioè che la moneta sia onesta avendo fatto quella certa osservazione. Secondo il teorema di Bayes tale probabilità è:  $P(H|O) = P(O|H) * P(H) / P(O)$ . Tralascio i dettagli matematici e mi concentro su ciò che il teorema dice: esso ci dice come calcolare la probabilità che l'ipotesi sia corretta, data un'osservazione. In altre parole: ci dice come verificare se una teoria sul mondo reale è vera oppure no.

Le esperienze di Graham dicono che il suo filtro è esatto al punto di mancare solo 5 messaggi di spam ogni 1000, senza alcun falso positivo, cioè messaggi che non sono spam ma vengono identificati come spam (inutile precisare che questo è il lato peggiore di tutti i tipi di filtro). I filtri più diffusi funzionano in base alle proprietà individuali di un singolo messaggio, ma l'approccio statistico su insiemi di messaggi è migliore. Si parte con un insieme di messaggi di spam e uno di messaggi che non sono spam. Si effettua una scansione contando il numero di volte che ogni parola appare in ogni insieme, ottenendo così due tabelle che indicano quali sono gli esemplari di parole e il numero delle loro apparizioni. Una terza tabella viene generata e riporta ogni esemplare di parola e la probabilità che un messaggio che la contiene sia spam. In pratica, si distinguono le parole che appaiono solo nei messaggi di spam e quelle che solo occasionalmente appaiono anche in messaggi legittimi. Quando arriva un nuovo messaggio, viene calcolata la probabilità che esso sia spam. Quando si incontrano parole nuove, si assegna loro una probabilità arbitraria, considerando che molto probabilmente non sono tipiche dello spam, solitamente ripetitivo.

Al contrario di SpamAssassin, che assegna un punteggio, l'approccio bayesiano attribuisce un probabilità reale. Per esempio: la parola "sex" indica il 97% di probabilità che il messaggio che la contiene sia spam. "Sexy" il 99%. E un messaggio che le contiene entrambe avrà il 99.97% di probabilità di essere spam. Ma se lo stesso messaggio contiene parole che raramente appaiono nello spam (come "though" or "tonight" or "apparently"), tale probabilità si abbassa. Queste probabilità vanno calcolate per ogni utente perché, se i messaggi di spam sono simili per tutti (a volte sono proprio gli stessi), quelli personali sono invece molti diversi, ma il filtro bayesiano ne tiene automaticamente conto.

### 7.2.6. L'utente reagisce: il reporting individuale e SpamCop

Nonostante le varie tecniche e i filtri si può comunque essere vittima dello spamming. In questo caso è opportuno reagire. In determinati casi si può ricorrere alla legge, come illustrato nel capitolo precedente e cercare di creare delle difficoltà allo spammer. Purtroppo il ricorso alla legge ha molti limiti e rischia di essere costoso.

Una reazione possibile e spesso efficace è quella del reporting. La vittima può segnalare il caso di spamming al provider dello spammer, nella speranza che questo intervenga e prenda provvedimenti nei confronti del cliente che ha abusato delle sue strutture. Se il messaggio ha attraversato un server che fa da relay, allora si può chiedere all'amministratore di chiuderlo. Bisogna però avere una certa conoscenza tecnica in modo da poter individuare il server e-mail reale da cui è partito il messaggio di spam. In certi casi, può essere opportuno segnalare il caso anche a provider implicati indirettamente: alcuni ISP (soprattutto quelli di grandi dimensioni), infatti, non apprezzano che il loro nome venga usato illegittimamente.

Se si desidera intraprendere la strada della segnalazione autonoma al provider dello spammer è necessario avere a disposizione alcuni strumenti. Esistono in Rete alcuni siti che offrono dei tool che aiutano a identificare la reale provenienza di un messaggio. In sostanza, bisogna disporre degli header completi del messaggio, di un modo per tradurre i numeri IP in domini e di un accesso agli archivi Whois. Un sito che offre questi tool è UYN Spam Combat<sup>28</sup>, dove si possono consultare diversi archivi di numeri IP e verificare la presenza di un server e-mail in qualche blacklist in Rete (sulle blacklist, o RBL, si veda anche il capitolo 7.3.). Per quest'ultima operazione, uno dei siti più completi è drbcheck<sup>29</sup> perché permette, con un solo clic, di consultare decine di blacklist e di archivi on-line. Un sito storico è SamSpade<sup>30</sup> che propone molti strumenti ed è molto semplice da usare.

Uno dei modi più semplici ed efficaci per segnalare lo spam ricevuto ai provider interessati è SpamCop<sup>31</sup>, gestito da Julian Haight. SpamCop è composto da tre servizi. Il primo è il Reporting Service, grazie al quale chiunque, gratuitamente, può inviare a SpamCop i messaggi di spam che riceve e reclamare con l'amministratore interessato. Ci torneremo tra poco. I rapporti del Reporting Service generano una serie di dati che alimenta una banca dati alla base del Blocking Service. Questo è un servizio a pagamento che può essere usato dagli amministratori di server e-mail analogamente ai sistemi di blacklist descritte più avanti. Il Blocking Service, inoltre, serve

---

<sup>28</sup> UYN Spam Combat, <http://combat.uyn.com/>.

<sup>29</sup> drbcheck, <http://moensted.dk/spam/>.

<sup>30</sup> SamSpade, <http://samspade.org/>.

<sup>31</sup> SpamCop <http://www.spamcop.net/>.

direttamente al Mail Service, un altro servizio a pagamento che prevede l'offerta di acconti di posta filtrati dallo spam.

Grazie al Reporting Service, SpamCop riceve moltissimi messaggi di spam ogni giorno. Ognuno di questi messaggi viene analizzato automaticamente e viene creato un messaggio di reclamo che verrà inviato agli amministratori di sistema coinvolti dallo spammer, anche a loro insaputa. SpamCop propone all'utente una serie di indirizzi a cui mandare la protesta, ed è responsabilità dell'utente scegliere se inviarli e a chi tra gli indirizzi proposti. L'indirizzo mittente del reclamo è un indirizzo anonimo di SpamCop, tuttavia eventuali repliche dell'amministratore verranno reindirizzate all'utente che ha segnalato il messaggio. L'amministratore "colpevole", normalmente, non sa nulla dello spammer ed è interessato a sapere se qualcuno abusa dei suoi sistemi. È quindi probabile che chiuderà l'acconto dello spammer, se è effettivamente in grado di identificarlo. I messaggi di reclamo sono cortesi e riportano le informazioni di cui l'amministratore ha bisogno per identificare lo spammer.

Una reazione dell'utente potrebbe essere stimolata da una taglia, come proposto<sup>32</sup> dall'esperto di diritto Lawrence Lessig. La legge dovrebbe imporre agli spammer di rendere riconoscibili i loro messaggi e li costringerebbe a pagare una taglia cospicua, se non si comportano correttamente, al primo utente che segnala uno spam non conforme. Lessig ci crede talmente che ha scommesso il suo posto di lavoro<sup>33</sup>.

### 7.3. Strumenti per l'amministratore di server e-mail

Gli amministratori di server e-mail sono responsabili del corretto funzionamento dei sistemi di posta elettronica. Ne troviamo presso i provider e presso le aziende o le istituzioni che hanno un proprio server e-mail visibile su Internet. I problemi con cui sono confrontati sono simili indipendentemente dal tipo di ente per cui lavorano: proteggere i propri utenti e i propri sistemi dall'inondazione di spam ed evitare di diventare fonte di spam da parte di propri utenti o di esterni che sfruttano i propri sistemi. Naturalmente vi sono anche delle differenze e la situazione cambia a seconda della dimensione: i responsabili dei sistemi di posta elettronica di un provider di grosse dimensioni, con decine o centinaia di migliaia di clienti, non potranno comportarsi con la stessa flessibilità di un amministratore di server di un'azienda con un centinaio di utenti.

---

<sup>32</sup> Lawrence Lessig, *A bounty on spammers*, 16 settembre 2002, in CIO Insight, <http://www.cioinsight.com/article2/0,3959,533225,00.asp> (consultato il 7 gennaio 2003).

<sup>33</sup> Lawrence Lessig, *Putting my job where my mouth is*, 1 gennaio 2003, in Lessig Blog, [http://cyberlaw.stanford.edu/lessig/blog/archives/2003\\_01.shtml#000787](http://cyberlaw.stanford.edu/lessig/blog/archives/2003_01.shtml#000787) (consultato il 7 gennaio 2003).

Tutti, però, devono tenersi informati su ciò che accade. Per questo esistono molti siti che trattano l'argomento in modo approfondito e con competenza.

Un amministratore responsabile, inoltre, cercherà di informare i propri utenti sui sistemi anti-spam installati, lasciando loro la scelta se usarli o no, e li educerà sul modo di installare e configurare i filtri locali. Gli utenti invece dovrebbero cercare di informarsi sugli usi e sui costumi della Rete per sapere a cosa vanno incontro se intendono pubblicare il proprio indirizzo di posta elettronica su pagine web o sui forum.

I provider, o comunque coloro che amministrano un server e-mail, hanno un grande interesse a ridurre il problema dello spamming perché, come visto precedentemente, esso è fonte di numerosi problemi, che si traducono in costi. Alcuni piccoli provider<sup>34</sup> stimano che i danni arrivino fino a 20 dollari all'anno per utente, cioè il 10% del costo per mantenere operativo il server e-mail. AOL Time Warner dichiara<sup>35</sup> di spendere il 15%, mentre AT&T specifica una spesa di 35.000 dollari al mese nella lotta allo spamming. Se per l'utente finale lo spamming è una noiosa seccatura, il provider si accorge di tutte le conseguenze negative: blocchi di sistema dovuti all'intasamento, dischi che si riempiono, reclami da parte di utenti.

Esiste un documento, preparato dal RIPE<sup>36</sup> (Réseaux IP Européens) che raccoglie alcuni consigli per aiutare gli amministratori di sistema. In particolare, si ricorda che il sistema non deve permettere il relay a terzi e deve inserire nei messaggi in uscita le informazioni che servono a risalire al mittente. L'amministratore, inoltre, deve collaborare e dar seguito alle richieste di collaborazione o alle segnalazioni provenienti dall'esterno, deve intervenire in caso di abuso provato, deve fornire informazioni sui provvedimenti presi e deve educare i propri utenti al fenomeno dello spamming.

### 7.3.1. Filtri in uscita e in entrata

Il provider deve preoccuparsi innanzitutto di non essere fonte, anche involontariamente, di spam. Uno dei modi per farlo consiste nell'installare filtri in uscita. Questo viene già applicato da molti provider, soprattutto da quelli di grandi dimensioni. I server e-mail vengono configurati in modo da impedire invii massicci di messaggi di posta elettronica da parte dello stesso utente, soprattutto nelle connessioni gratuite in dial-up (per un approfondimento su questo tipo di soluzione rimando al capitolo 7.4.1). Un altro modo di evitare di essere fonte di spam è quello

---

<sup>34</sup> **Mitch Wagner**, *ISP Chief: Spam Is 'A Thousand Times More Horrible Than You Can Imagine'*, 19 dicembre 2002, in InternetWeek.com, <http://www.internetwk.com/story/INW20021219S0003> (consultato il 20 dicembre 2002).

<sup>35</sup> **Sharon Gaudine Suzanne Gaspar**, *The Spam police*, 10 settembre 2001, in Network World, <http://www.nwfusion.com/research/2001/0910feat.html> (consultato il 30 dicembre 2002).

<sup>36</sup> **RIPE**, <http://www.ripe.net/>. Il documento è: **Richard Clayton**, *Good practice for combating Unsolicited Bulk Email*, 18 maggio 1999, <http://www.ripe.net/ripe/docs/ripe-206.html> (consultato il 2 gennaio 2003).

di chiudere tutti i server al relay da parte di terzi, anche se questa soluzione viene talvolta contestata: in certe situazioni (un cliente ha bisogno di accedere dall'esterno per inviare posta) un server aperto può essere necessario. Esistono soluzioni che consentono di usare il server e-mail anche dall'esterno, senza che per questo resti aperto a chiunque: ci sono dei client e server per la posta che supportano un'autenticazione basata su un nome utente e una password. In alternativa si può istruire il server e-mail a permettere il relay da parte di un numero IP dal quale è stata lanciata, immediatamente prima, una sessione POP valida. In altre parole, l'utente deve controllare la sua posta prima di usare il server e-mail per spedirne altra. Visti i rischi enormi che si affrontano lasciando un server aperto al relay da parte di terzi, e visto che le situazioni in cui può servire sono poche e comunque esistono alternative, personalmente credo che non vi sia necessità di lasciare aperti i server.

Per quanto riguarda la protezione dallo spamming proveniente dall'esterno, la soluzione è quella di applicare qualche tipo di filtro, analogamente a quelli descritti per l'utente finale. I filtri agiranno secondo dei criteri stabiliti. Chi gestisce il server di posta può usare un prodotto che filtra i messaggi esternamente e poi li recapita sulla sua rete oppure può configurare il software in modo da utilizzare una blacklist disponibile in Rete. Inoltre è possibile predisporre delle configurazioni direttamente sul proprio server, in modo che i messaggi in cui c'è qualcosa di "sbagliato", caratteristica che identifica molti spam, vengano intercettati. Tale sistema può funzionare anche per evitare il relay da parte di terzi: si cercano i messaggi provenienti da IP esterni e diretti a IP esterni e i messaggi provenienti da domini inesistenti o contenenti irregolarità nel protocollo SMTP. Come gli utenti, anche i provider possono realizzare liste di IP, di nomi di dominio o di nomi utenti personalizzati secondo le loro esigenze.

La pratica di filtrare la posta a livello server sembra in contrasto con il diritto civile relativo alla libertà di corrispondenza epistolare, sancito sia nella costituzione svizzera che in quella italiana<sup>37</sup>. Non è permesso limitare la corrispondenza personale di un individuo. Il mancato recapito di messaggi legittimi (falsi positivi) perché erroneamente scambiati per spam potrebbe portare a conseguenze legali negative per il provider. Appare quindi necessario che, se il provider decide di utilizzare filtri sulla posta in entrata, informi i suoi clienti ed eventualmente dia loro la possibilità di scegliere se usarli o meno. I problemi causati dallo spamming giustificano comunque il ricorso ad alcune misure di protezione. Un comportamento prudente e ragionevole viene messo in atto dal provider italiano Spin, che spiega, su una pagina web dedicata<sup>38</sup>, quali filtri vengono applicati. Inoltre viene specificato che quando un messaggio

---

<sup>37</sup> **Giuseppe Briganti**, *Spamming e diritto - L'invio di messaggi di posta elettronica non richiesti*, 29 dicembre 2001, in Ius Reporter, <http://www.iusreporter.it/Testi/doc-spammin.g.htm> (consultato il 19 novembre 2002).

<sup>38</sup> **Spin**, *I filtri antispam di Spin*, [http://www.spin.it/spam/spam\\_filters.php3](http://www.spin.it/spam/spam_filters.php3) (consultato il 21 dicembre 2002).

viene identificato come spam, esso non viene cancellato, ma viene rimandato al mittente con la spiegazione di cosa è successo e di come si può contattare Spin tramite un form su web. Al cliente è comunque lasciata la possibilità di non utilizzare i filtri anti-spam.

### 7.3.2. Le RBL

Le RBL (Realtime Blackhole List o Relay Blocking list, o liste di blocco) sono certamente uno degli strumenti più usati e più discussi nella lotta contro lo spamming a livello di amministratori di sistema.

Tecnicamente la RBL funziona come in questo esempio: il server e-mail del nostro provider, quello dove risiede la nostra mailbox, viene contattato da un altro server e-mail che desidera inviare un messaggio. Il nostro server e-mail, prima ancora di vedere il messaggio, chiede alla RBL se il server che lo sta contattando è presente nell'elenco. Se la risposta è positiva, il nostro server non accetterà nemmeno la connessione. Viene quindi esaminata la provenienza dei messaggi e non i messaggi stessi. È inoltre il nostro provider a decidere se utilizzare o meno una RBL. E questa decisione concerne le mailbox di tutti gli utenti del provider, utenti che spesso non sono a conoscenza di questi filtri.

Vedremo alcuni esempi di RBL, di cui esistono in Rete numerose versioni gratuite o a pagamento. Vale però la pena iniziare con l'approfondire alcuni concetti alla base delle RBL.

Mentre i gestori delle RBL sostengono che ogni amministratore di server e-mail è libero di scegliere se usare o meno i servizi offerti, chi si oppone ritiene che le RBL siano un'entità nascosta dotata di un grande potere. Il paragone è quello della linea telefonica: chi accetterebbe un'entità che decide con criteri poco chiari chi può telefonarci e chi no, e che per di più non si sa con precisione da chi è gestita?

Ma il punto cruciale attorno a cui ruotano i dibattiti, più o meno esplicitamente, è quello relativo ai criteri con cui i server e-mail finiscono nelle RBL. Solitamente le RBL elencano i server che sono aperti al relay da parte di terzi. Non tutti i server aperti al relay, però, sono fonte di spam. I gestori delle prime RBL inserivano nei loro elenchi solo i relay aperti fonte di spam. Oggi sembra che sia molto facile finire negli elenchi di alcune RBL, e molto difficile uscirne. Alcuni provider sostengono di essere finiti nelle RBL per ritorsione, perché avevano rifiutato i messaggi che cercavano di provare dall'esterno se i loro server e-mail erano aperti al relay o no. Infatti, è questo il sistema usato dalle RBL per verificare se un server e-mail è aperto al relay: viene mandato un messaggio dal server della RBL a se stesso, sfruttando il server e-mail sospetto. Se il messaggio effettivamente arriva, significa che il server e-mail sospetto è aperto al relay. Tra l'altro, alcuni ritengono che questa pratica sia illegale negli Stati Uniti, ma non esistono precedenti in tribunale.

Un'altra accusa di ritorsione arriva da quei provider che intervengono contro gli spammer, ma solo nel giro di qualche giorno. Troppo, per i gestori di alcune RBL, che li inseriscono quindi nella loro lista.

Il danno più grande derivato dall'uso delle RBL è quello di escludere utenti legittimati che hanno la sfortuna di dover utilizzare server e-mail aperti, anche se questi non vengono usati da spammer. Questi utenti vedranno spesso i loro messaggi respinti. È il problema dei falsi positivi, di cui parla Paul Graham<sup>39</sup> citando uno studio<sup>40</sup>: MAPS intercetterebbe solo il 24% dei messaggi di spam, generando il 34% di falsi positivi. Secondo Graham e altri, è il concetto alla base del metodo di MAPS a renderlo così inefficiente: lo spam va identificato in base a criteri relativi al messaggio e non in base al server di provenienza. Sono davvero molti gli esempi in cui intere aziende sono state tagliate fuori dalla Rete, con danni economici non indifferenti, per un disguido o un errore di configurazione. Il problema delle RBL è che considerano il sospetto come un colpevole fino a prova contraria. A volte sono delle punizioni preventive.

Dal canto loro, i gestori delle RBL replicano cercando di dimostrare che si fa tutto il possibile per elencare solo i server effettivamente colpevoli e ricordando che l'uso della lista non è imposto ma dipende totalmente dalla scelta dell'amministratore di sistema. Essi sostengono anche che non ci sono alternative se gli amministratori dei server e-mail incriminati non rispondono agli avvisi e alle richieste di collaborazione, e quindi diventa necessario intervenire drasticamente. Causando anche danni agli utenti innocenti, questi protesteranno mettendo gli amministratori sotto pressione. È il caso dei server e-mail cinesi, coreani o più in generale asiatici: alcune RBL elencano interi blocchi di indirizzi IP di questi Paesi perché gli ISP locali non offrono collaborazione e i loro server sono fonti di spam importanti. Escludere un intero Paese in questo modo è un atto molto drastico, che mette in pericolo i principi di libertà e democrazia alla base di Internet, soprattutto perché deciso da piccoli gruppi di persone. L'applicazione del motto "à mali estremi, estremi rimedi" diventa discutibile, anche se alcune cifre (50.000 messaggi di protesta per spam inviati quotidianamente a China Telecom da tutto il mondo, senza alcuna risposta<sup>41</sup>) sembrano confermare la visione dei gestori delle RBL.

Il punto, per un amministratore, resta comunque sempre la protezione dei propri utenti e dei propri sistemi. Può utilizzare filtri sul server e diverse RBL, ma deve prestare attenzione a non escludere troppi segmenti di Rete. Visto che filtri e RBL sono soluzioni drastiche, è

---

<sup>39</sup> **Paul Graham**, *Filters vs. Blacklists*, settembre 2002, <http://www.paulgraham.com/falsepositives.html> (consultato il 30 dicembre 2002).

<sup>40</sup> **Sharon Gaudine Suzanne Gaspar**, *The Spam police*, op. cit.

<sup>41</sup> **Michelle Delio**, *Not all Asian E-Mail is spam*, 19 febbraio 2002, in *Wired News*, <http://www.wired.com/news/politics/0,1283,50455,00.html> (consultato il 2 gennaio 2003).

consigliabile utilizzarli solo quando il problema diventa pressante e urgente, e molti utenti si lamentano.

Uno dei problemi conseguenti all'uso delle RBL è che chi le usa spesso si preoccupa solo della configurazione del proprio server e non è informato sui dettagli relativi alla gestione della RBL stessa. Questo peggiora le cose: può capitare che un provider non sappia che una RBL lo isola nei confronti di un intero Paese come la Cina o la Corea.

Chi si oppone usa spesso toni idealistici: le soluzioni sarebbero da ricercare in soluzioni globali la cui configurazione va lasciata all'utente (privato o azienda) che va educato ad affrontare il fenomeno. La soluzione migliore è quella di boicottare i prodotti pubblicizzati tramite spamming in modo da rendere questa pratica economicamente poco interessante. Alcuni, come John Gilmore (cofondatore della Electronic Frontier Foundation), sostengono<sup>42</sup> inoltre che si dovrebbe avere il diritto di tenere il proprio server e-mail aperto al relay (ma fanno comunque di tutto per non lasciarlo in balia degli spammer).

Come anticipato, nei prossimi capitoli vedremo alcuni esempi di RBL esistenti in Rete.

### 7.3.3. MAPS: Mail Abuse Prevention System

La missione del MAPS<sup>43</sup> (Mail Abuse Prevention System), un'organizzazione californiana, è quella di difendere il sistema di posta elettronica su Internet dagli abusi degli spammer. I mezzi usati sono quelli dell'educazione e dell'incoraggiamento degli ISP a rinforzare le condizioni di servizio proibendo ai loro clienti di praticare abusi via e-mail. Per raggiungere i suoi obiettivi, il MAPS mette a disposizione (a pagamento) tre liste di blocco. I promotori di MAPS tengono a dire che chi usa le liste lo fa di propria volontà e dev'essere cosciente che grazie ad esse può rifiutare anche messaggi legittimi perché anche i network "cattivi" possono ospitare utenti "buoni".

Nella MAPS Realtime Blackhole List (MAPS-RBL) vengono elencati, attraverso i loro numeri IP, quei network che fanno parte di Internet, noti per avere al loro interno degli spammer particolarmente attivi. I network inseriti in questa lista non possono scambiare dati con i network che fanno uso della lista. La MAPS-RBL viene usata in particolare per i network che sono all'origine di spam (per esempio, i relay aperti di tipo multi-hop), per quelli che fanno da relay a spammer oppure offrono qualche tipo di supporto (hosting di pagine web, fornitura di risorse come DNS, e-mail, eccetera). Chi decide di usare la RBL per evitare di ricevere spam sceglie spontaneamente di non scambiare traffico con i blocchi di indirizzi elencati nella lista.

---

<sup>42</sup> **Stewart Taggart**, *Spam Blockers Pass It On*, 2 luglio 2001, in Wired, <http://www.wired.com/news/culture/0,1284,44876-2,00.html> (consultato il 30 dicembre 2002).

<sup>43</sup> **MAPS**, <http://www.mail-abuse.org/>.

Lo scopo di questa lista è quello di scoraggiare i provider a fornire connettività e servizi agli spammer.

La stessa cosa succede per la MAPS Dial-up User List (MAPS-DUL). Questa elenca blocchi di indirizzi IP caratteristici di accessi in dial-up o simili, vale a dire indirizzi IP che vengono assegnati dinamicamente all'utente che si collega temporaneamente a un certo provider. Alcuni network decidono di non ricevere messaggi da tali blocchi perché spesso all'origine di spam. Gli utenti che sfruttano questo tipo di accesso dovrebbero usare il server e-mail che l'ISP mette a disposizione. Questa lista ha l'obiettivo di educare i provider a fornire un accesso a Internet in modo responsabile ai clienti.

L'ultima lista di blocco si chiama MAPS Relay Spam Stopper (MAPS-RSS) e consiste di una banca dati di IP di server e-mail a relay aperto. Chi amministra un server e-mail può utilizzare questa lista per rifiutare messaggi dai server aperti.

Queste tre liste vengono compilate e aggiornate dai promotori del MAPS e dagli utenti che inviano segnalazioni.

Data la natura drastica di questi filtri, il MAPS viene spesso accusato di praticare censura e di limitare la libera comunicazione su Internet. Infatti, come detto, può addirittura essere illegale impedire a un utente di ricevere posta a lui diretta. Di sicuro è una soluzione drastica che però potrebbe essere l'unica possibile in tempi brevi.

Recentemente MAPS ha introdotto la MAPS Non-confirming Mailing List (MAPS-NML), cioè una lista di numeri IP per i quali è dimostrato che ospitano mailing list gestite scorrettamente, cioè che non richiedono conferma al momento dell'iscrizione e pertanto sono soggette ad abusi.

#### **7.3.4. Spamhaus**

Spamhaus<sup>44</sup> è un servizio simile a MAPS che tenta di tenere una traccia dei peggiori spammer, delle gang di spammer e dei servizi che supportano lo spam. Lavora con i provider per identificare e rimuovere gli spammer più recidivi da Internet. La Spamhaus Block List (SBL) è una lista di indirizzi IP di spammer che viene utilizzata da network aziendali in tutto il mondo e protegge, secondo alcune stime, 100 milioni di mailbox da fonti di spam persistenti. Il secondo servizio offerto da Spamhaus è il Register Of Known Spammer Operations (ROKSO): in esso vengono elencati gli spammer che sono stati espulsi dai provider tre volte o più. Sono un centinaio e molti di questi sono anche stati indagati per truffa o frode. A loro dobbiamo più del 90% di spam americano ed europeo. ROKSO incrocia le informazioni e le prove di ogni

---

<sup>44</sup> Spamhaus, <http://www.spamhaus.org/>.

operazione di spam per assistere gli helpdesk dei provider e chi mantiene le liste di blocco. L'uso di questi servizi è gratuito. Anche Spamhaus avvisa che l'uso delle sue liste può portare al blocco di messaggi legittimi e si difende dalle accuse di censura in modo simile a quanto fa il MAPS. Il sito UXN Spam Combat, usato per l'esempio di analisi di header del capitolo 3.5., è un servizio di Spamhaus.

### **7.3.5. SPEWS: Spam Prevention Early Warnign System**

SPEWS<sup>45</sup> (Spam Prevention Early Warnign System) è una lista gestita anonimamente da amministratori di sistema sparsi per il mondo. Si tratta di una gestione a tolleranza zero, che elenca i blocchi di IP dei provider che offrono protezione agli spammer. Data l'intransigenza applicata, l'arrivo di SPEWS nel panorama della lotta allo spamming ha segnato un passo importante: molti ISP si sono trovati costretti a escludere gli spammer per evitare di finire nella lista, dalla quale è abbastanza difficile uscirne. I provider che desiderano usare la lista di SPEWS possono farlo gratuitamente e possono scegliere due livelli di utilizzo: il primo livello esclude solo i blocchi di indirizzi IP che sono stati usati da uno spammer, mentre il secondo comprende anche quelli sospettati di essere usati. Inutile dire che in questo secondo caso il pericolo di falsi positivi è molto alto.

### **7.3.6. ORDB: Open Relay DataBase**

ORDB<sup>46</sup> (Open Relay DataBase) è una banca dati di server e-mail a relay aperto contenente oltre 200.000 indirizzi IP. È situato in Danimarca ed è uno dei numerosi eredi di ORBS, storica banca dati di relay aperti chiusa nel 2001 dopo che due aziende neozelandesi avevano vinto una causa legale contro l'amministratore di ORBS, che aveva sede in Nuova Zelanda, per averle inserite nella banca dati ORBS, tra l'altro, era stato al centro di una disputa con MAPS: ORBS aveva accusato MAPS di averla inserita nelle sue liste di blocco per ragioni finanziarie, MAPS aveva replicato che ORBS stava attaccando i suoi sistemi. Gli altri due eredi di ORBS erano ORBL (Open Relay BlackList, in Arizona) e ORBZ (Open Relay Black Zone, in Inghilterra), ora chiusi.

Tornando a ORDB, esso può essere usato liberamente e gratuitamente con diversi tipi di server e-mail. Come fanno i gestori di MAPS, anche quelli di ORDB avvisano che l'uso della lista potrebbe bloccare messaggi legittimi. Sul sito sono presenti moltissime spiegazioni, parzialmente anche in italiano, sulla configurazione dei propri sistemi in modo che essi sfruttino la banca dati di ORDB.

---

<sup>45</sup> Spews, <http://www.spews.org/>.

<sup>46</sup> ORDB, <http://www.ordb.org/>.

### 7.3.7. Altri prodotti commerciali

Tra i prodotti anti-spam rivolti agli amministratori di sistema più diffusi vi sono quelli di Brightmail e di MessageLabs.

Brightmail è un'azienda americana che gestisce una rete di indirizzi-trappola, in cui finiscono migliaia di messaggi di spam ogni ora. Grazie a questo immenso archivio in continua evoluzione, Brightmail può installare presso le reti dei suoi clienti una serie di filtri che intercettano i messaggi di spam in base al risultato in tempo reale del suo network di prova. In concreto, un server e-mail viene posto tra i sistemi del cliente e Internet e tutta la posta passa attraverso questo sistema, dove intervengono i filtri aggiornati continuamente. Bluewin, il provider svizzero del gruppo Swisscom, mette a disposizione dei clienti che lo desiderano il filtro di Brightmail.

MessageLabs invece è inglese e vende un servizio basato su un sistema euristico, che impara dall'esperienza. Viene utilizzata l'intelligenza artificiale per creare ed espandere la base di conoscenze usata per identificare lo spam proveniente da Internet. È un sistema rapido che esamina il contenuto dei messaggi e decide, in base ad alcuni criteri, un punteggio oltre il quale il messaggio viene classificato come spam e quindi eliminato.

### 7.3.8. I filtri web: Hotmail

Non ho avuto l'opportunità di provare i filtri direttamente. Una prova indiretta viene però dal servizio offerto da Hotmail, che consiste in un indirizzo di posta elettronica consultabile da web, con filtro anti-spam. Nelle pagine relative alla configurazione del proprio indirizzo, è possibile impostare un livello di protezione contro lo spam e decidere cosa fare dei messaggi intercettati: cancellarli o metterli in un'apposita cartella per un successivo controllo. Esistono tre livelli di protezione: se si sceglie quello chiamato "Predefinito" viene eliminata solo la posta palesemente indesiderata. Con il livello "Esclusivo" invece vengono recapitati solo i messaggi provenienti da indirizzi presenti nella lista dei contatti personali. Con il livello medio, definito "Alto", dovrebbe venire bloccata la maggior parte della posta indesiderata. Non sembra però che il sistema funzioni molto bene: l'ho provato sull'indirizzo Hotmail *mimi1080@hotmail.com*, creato per ricevere messaggi di spam. Dal 14 agosto 2002 al 29 dicembre 2002, ho ricevuto 618 messaggi in "Posta in Arrivo", tutti di spam, mentre quelli deviati in "Posta indesiderata" sono solo 240. Il filtro di Hotmail quindi si dimostra poco utile e particolarmente inefficace: controllando la provenienza di un certo numero di messaggi scelti a caso ci si rende conto che provengono da server segnalati su numerose RBL.

Sembra che altri servizi, che non ho provato direttamente, funzionino meglio. Per esempio, quello offerto da Yahoo prevede un feedback da parte dell'utente, che può segnalare facilmente

un messaggio di spam sfuggito all'intercettazione dei filtri. In questo modo il sistema "impara" dall'esperienza degli utenti.

## 7.4. Soluzioni a lungo termine

Le soluzioni disponibili per l'utente e quelle per gli amministratori di server e-mail hanno tutte il grande svantaggio di essere soltanto delle contromisure: tentano di arginare il fenomeno in attesa che gli spammer trovino altre vie. A quel punto, si cercheranno altri modi per affrontare la nuova forma che il fenomeno dello spamming avrà assunto.

Il già citato Brad Templeton<sup>47</sup> ha cercato di proporre alcune soluzioni a lungo termine che permettano di eliminare lo spamming all'origine. Le soluzioni finora presentate non devono però essere trascurate: esse sono la prima, e per ora unica, difesa.

Templeton, come presidente della Electronic Frontier Foundation, è molto attento alla tutela dello scambio di messaggi privati e ai diritti civili che la nostra società riserva a tutti. Nella battaglia contro lo spamming è necessario trovare un equilibrio tra chi desidera comunque comunicare normalmente e chi invece vuole imporre limitazioni eccessive. Purtroppo si trovano persone o gruppi che hanno radicalizzato la lotta allo spamming, eccedendo in posizioni estreme e tentando di ostacolare tutti coloro che non sono pienamente d'accordo con loro. Tali gruppi, forse strumentalizzati, pretendono controlli ferrei e punizioni esemplari per chi trasgredisce. Ma è necessario ricordare che la nostra è una società libera che prevede la libera comunicazione, e quindi anche il diritto di comunicare con gli sconosciuti. Il problema è l'abuso del diritto di comunicare da parte degli spammer, ma la soluzione non è quella di abolire o impedire la comunicazione libera. Gli americani dicono che il primo emendamento (quello che, nella loro costituzione, garantisce la libertà d'espressione) non è solo una legge, è anche una buona idea. La conclusione è che dobbiamo combattere lo spamming nel modo meno restrittivo possibile, proteggendo la comunicazione normale uno-a-uno (anche se a volte ci disturba).

Contemporaneamente è importante arrivare a una definizione del problema a livello legislativo, in modo da poter introdurre una soluzione a lungo termine. Per questo scopo è importante sostenere le associazioni attive nella lotta e nell'informazione, in modo da portare il dibattito anche all'esterno del mondo tecnico che attualmente se ne sta occupando.

### 7.4.1. Server che strozzano

Ho già accennato alla possibilità, per i provider, di filtrare i messaggi in uscita, di limitare cioè la quantità di messaggi che un cliente può inviare contemporaneamente. Questa soluzione

sarebbe veramente efficace solo se tutti i provider del mondo, nessuno escluso, la adottassero. Ne basta uno che non collabori e il problema dello spamming non viene risolto. Esiste però un meccanismo di questo tipo in grado di funzionare. La collaborazione di tutti i provider non sarebbe immediata, ma a lungo termine il rischio di restare esclusi dalla Rete li porterebbe ad aderire.

Alla base di questo sistema vi è un contratto tra il provider e il cliente. Tale contratto deve chiaramente vietare lo spamming e, in caso di abuso, prevedere l'interruzione immediata di tutti i servizi e un risarcimento cospicuo per l'ISP. Già oggi le condizioni di servizio previste da molti provider prevedono clausole di questo tipo. Il problema, oggi, è che non sempre si può rintracciare il cliente che ha abusato, soprattutto nel caso di connessioni dial-up gratuite, anonime o di prova, per le quali ci si iscrive online e si possono fornire dati fasulli in quanto non viene verificata preventivamente l'identità dell'utente.

Il sistema proposto da Templeton prevede delle limitazioni nel servizio finché il contratto non viene accettato e il cliente non prova la propria identità. Le pratiche di iscrizione online o di offerte di prova non vengono ostacolate.

La limitazione consiste nell'obbligo di usare esclusivamente un server e-mail apposito per mandare i messaggi di posta elettronica. Templeton chiama questi server throttle: server che strozzano. Lo scopo è di fare in modo che gli utenti non possano mandare messaggi di massa, a meno che non possano essere rintracciabili e perseguibili in caso di abuso, senza impedire o limitare l'uso dei messaggi individuali.

Tecnicamente, l'utente che non ha ancora accettato il contratto (perché non vuole o perché non l'ha ancora fatto) dev'essere distinto dagli altri clienti negli archivi del provider e i router vanno programmati in modo da impedire l'uso della porta SMTP su server e-mail diversi da quello dedicato.

La chiave di questo meccanismo sta nel server dedicato, presente presso l'ISP o da qualche parte in Rete (infatti può essere anche un open relay, in quanto limita la massa di messaggi e non può, per questa ragione, diventare un catalizzatore di spam). Presso questo server, ogni utente ha a disposizione un limitato volume di messaggi abbastanza alto per soddisfare i bisogni normali di un individuo, ma sufficientemente basso per eliminare gli invii di massa. Probabilmente una piccola parte di messaggi di spam verrà comunque inviata sulla Rete, ma non in quantità eccessiva da creare troppo disturbo.

Questo metodo soddisfa anche i difensori dei diritti civili, perché è possibile l'uso dei remailer anonimi, che inoltrano i messaggi nascondendo l'identità del mittente. Chi desidera

---

<sup>47</sup> Brad Templeton, *Essays on Junk E-mail (Spam)*, op. cit.

mandare messaggi anonimi di massa non potrà farlo attraverso i throttle server, ma potrà sempre accordarsi con una terza parte che accetti di nascondere la sua identità e si assuma la responsabilità per eventuali abusi. Dal punto di vista della difesa dei diritti civili, inoltre, questo sistema migliora di molto la situazione rispetto a quello delle blacklist. Il vantaggio di questa soluzione è che dovrebbe funzionare discretamente in tutti i Paesi, senza richiedere nuove leggi.

È possibile che un provider non possa o non voglia usare il sistema del throttle server. In questo caso, gli altri provider possono costringere tutto il traffico in arrivo da quell'ISP a passare attraverso un throttle server. È possibile farlo con un trucco sui DNS. Il domain name system permette ai server che ricevono posta di specificare una lista di server e-mail che accettano la loro posta (nel campo MX). Tale lista è compilata in base alle priorità. Normalmente la priorità più alta è assegnata al server e-mail reale, mentre gli altri sono dei sistemi di backup. Il provider che desidera fermare lo spam che riceve creerà un record MX con l'indicazione, ad alta priorità, del throttle server. L'inconveniente per chi è costretto a usare il throttle server consiste soltanto in qualche minuto di ritardo quando i messaggi personali vengono recapitati. Il vantaggio è che i messaggi di massa vengono filtrati ed eliminati. Se il provider da cui viene il messaggio fa parte del gruppo che ha acconsentito di essere responsabile per lo spamming, allora non dovrà passare attraverso il throttle server e manderà la posta direttamente, come oggi. Il throttle server verrà configurato in modo da rifiutare le connessioni provenienti dagli host autorizzati, che quindi proveranno automaticamente sui server indicati negli MX seguenti. I provider che non hanno aderito al contratto dovranno per forza usare il throttle server, perché gli altri server e-mail rifiuteranno le connessioni non autorizzate usando per esempio delle black o whitelist, come si fa adesso. La differenza con le liste di blocco attualmente in circolazione è che queste nuove liste non rischierebbero di bloccare anche i soggetti legittimati, intervenendo solo con quelli che deliberatamente ignorano le regole normali delle liste MX.

I throttle server possono essere creati e gestiti da organizzazioni anti-spam, da ISP o da aziende nate appositamente. La loro gestione non dovrebbe essere particolarmente dispendiosa: non è necessario che l'hardware sia veloce perché è compito di questi server essere lenti. Questi server dovranno essere molti e poter comunicare tra loro: essi stipano la posta in arrivo in una coda per qualche minuto, controllano la provenienza raggruppando le varie fonti e rilasciano dei rapporti da distribuire agli altri throttle server. In questo modo lo spammer non può attaccare usando più throttle server contemporaneamente.

Il problema più grosso lo riscontreranno gli utenti di quegli ISP che non vogliono aderire alle policy anti-spam: la loro posta potrebbe essere molto lenta, soprattutto se presso lo stesso ISP opera uno spammer. Questo è un incentivo per tutti (utenti e provider) a sottoscrivere le

condizioni di servizio anti-spam. Questi utenti possono comunque richiedere l'accesso a un altro server SMTP senza per forza cambiare ISP.

Questo sistema potrebbe funzionare, visto che la comunità di Internet, quella che subisce quotidianamente i disagi causati dagli abusi di qualsiasi genere, ha già dimostrato di poter cooperare efficacemente.

Una soluzione simile, a livello locale, è usata da *init7*, provider svizzero, per gli utenti dial-up gratuiti e anonimi (<http://www.init7.net/anti-spam/>).

#### 7.4.2. Francobolli elettronici

Una soluzione talvolta proposta è quella della tassa sull'e-mail. Può sembrare una provocazione o comunque una cosa irrealizzabile tecnicamente, ma il modo in cui questa possibilità è stata affrontata da Templeton, e anche da altri, non è superficiale. Dopo che quest'idea ha fatto la sua apparizione, nel 1995, ora sono in pochi a sostenerla. Lo stesso Templeton ne ha riconosciuto il fallimento, dovuto soprattutto alla mancata introduzione di un sistema di micropagamenti standard e alla diffusione troppo limitata dell'uso della firma digitale. Alcuni aspetti che riguardano la libertà d'espressione rinforzano i dubbi su questo tipo di soluzione. Comunque, essendo spesso invocata, vorrei approfondirla.

Oggi si possono configurare i programmi di posta per rifiutare i messaggi provenienti da indirizzi sconosciuti, sia in base all'indirizzo sia in base a una firma digitale. Lo scopo di questo sistema è di permettere anche agli sconosciuti di scriverci, ma di risparmiarci gli abusi. Per la precisione, si tratterebbe di un pagamento per la struttura dell'e-mail: il fenomeno dello spamming è in crescita perché il sistema della posta elettronica è economico (è stato costruito per esserlo).

Il sistema dei francobolli elettronici (e-stamp) prevede che ogni messaggio arrivi con una stringa di byte che rappresenta una piccola somma. Questo francobollo non rappresenta la somma pagata a un ipotetico ufficio postale, ma il potenziale pagamento al destinatario da parte del mittente, per compensare il disturbo di ricevere messaggi non sollecitati. L'e-stamp è un assegno elettronico criptato e firmato digitalmente con algoritmi basati sulla crittografia a chiave pubblica, equiparabile a un assegno tradizionale. Esso è unico e ha una scadenza breve (qualche giorno), dopo la quale non può più venirne reclamato il pagamento. La somma che rappresenta è piccola, per esempio 10 centesimi di franco svizzero.

Per spiegare il funzionamento del sistema, propongo l'esempio di Templeton. Alice vuole scrivere a Bob. Nel suo messaggio è incluso un e-stamp, l'assegno elettronico che ordina alla banca di Alice di pagare una certa somma a Bob. L'e-stamp è firmato digitalmente per certificare che il messaggio provenga effettivamente da lei. Alice mette un francobollo su tutti i

messaggi che scrive. Bob, e tutti gli altri, rifiutano automaticamente i messaggi privi di francobolli (perlomeno quelli che arrivano da estranei). Quando Bob riceve il messaggio di Alice può reclamare con pochi clic il pagamento dell'e-stamp, trasmettendo l'ordine alla banca, oppure lasciar cadere la cosa. Siccome questo sistema è pensato per fermare gli abusi, Bob lascerà che il francobollo scada senza inoltrarlo alla banca perché il messaggio di Alice non è un abuso. Quindi, la maggior parte degli e-stamp di Alice verrà annullata e lei non pagherà quasi nulla per spedire la sua posta agli amici. Se invece Bob reclamasse il pagamento dell'e-stamp, la cifra pagata da Alice sarebbe comunque piccola, un rischio che lei può correre tranquillamente. In questo caso, probabilmente, lei non scriverebbe più a Bob perché lo riterrebbe un maleducato. Bob, da parte sua, non diventerebbe mai ricco reclamando il pagamento per e-stamp di tutti i messaggi che riceve, ma perderebbe rapidamente gli amici.

Riassumendo, gli e-stamp sulla normale posta privata verranno spesso lasciati scadere senza reclamarne il pagamento, a meno che non si voglia essere considerati dei maleducati; quelli sui messaggi di spam invece serviranno da deterrente: il costo elevato di 100.000 francobolli, piazzati su altrettanti messaggi promozionali o di spam, il cui pagamento viene effettivamente reclamato, costituirebbe un limite naturale allo spamming.

Il funzionamento di questo sistema viene rafforzato dal rapporto tra Alice e la banca: questa può autorizzare Alice a generare un certo numero di e-stamp solo se ha depositato una somma sufficiente per coprirli. In pratica, se Alice desidera mandare 50 messaggi in una settimana, dovrà depositare 5 franchi (che probabilmente non verranno reclamati). Un'azienda che desidera inviare 100.000 messaggi dovrà offrire una garanzia di 10.000 franchi, che invece probabilmente verranno spesi, a meno che i destinatari non apprezzino il messaggio.

La cosa interessante è che non sarebbe necessario usare gli e-stamp molto spesso: molte persone configureranno i loro programmi di posta per accettare messaggi senza francobollo da una serie di indirizzi di persone di cui si fidano. Gli e-stamp sono necessari solo per i messaggi che si mandano agli sconosciuti, in realtà abbastanza rari per le persone comuni. Il sistema potrebbe diffondersi rapidamente se le aziende lo introducessero garantendo per i loro dipendenti, o i provider per i clienti paganti, di cui quindi possono fidarsi, recuperando poi insieme all'abbonamento il costo per gli e-stamp eventualmente reclamati. Così verrebbe risparmiato all'utente finale l'onere di installare il software necessario.

Questo sistema garantisce anche la possibilità di spedire messaggi in forma anonima, ma vi sarebbero alcune difficoltà dovute al fatto che la banca, se non può sapere con chi sta trattando, ha bisogno di più garanzie.

Il sistema di francobolli elettronici non impedisce la normale operatività delle mailing list, ma il meccanismo di iscrizione andrebbe migliorato. La soluzione più semplice sarebbe quella

di istruire il proprio programma di posta per accettare i messaggi provenienti dalla lista, mentre, per la spedizione, i gestori delle liste dovrebbero configurarle in modo da accettare messaggi solo dagli iscritti, cosa che spesso già accade. Ci sarebbero comunque problemi di gestione per le liste o le newsletter amatoriali, gestite da privati che non hanno né le competenze tecniche per adeguarsi alla soluzione, né la disponibilità finanziaria per garantire l'eventuale reclamo di migliaia di e-stamp.

Nonostante il sistema, una volta configurato e automatizzato, sia semplice da usare sia da parte del mittente che del destinatario, esso richiede comunque una nuova generazione di programmi di posta, la creazione di un'infrastruttura per la firma digitale e di una per i micropagamenti. Per queste infrastrutture i protocolli esistono, ma i vari tentativi di diffonderli su larga scala non hanno avuto successo: spesso i costi per l'utente finali sono troppo alti e non esiste interoperabilità fra strutture di diversi produttori.

Come detto, i sostenitori di questo sistema sono sempre meno convinti perché esso è troppo complesso e costituisce un ostacolo alla normale comunicazione. Per esempio, chi scrive con un francobollo elettronico a un gruppo di discussione Usenet per chiedere un favore impone a chi vuole aiutarlo il rischio di dover sborsare dei soldi per prestare il proprio aiuto. Le limitazioni imposte alla normale comunicazione (soprattutto fra sconosciuti) sono troppe. Inoltre, e questo è un punto molto importante, nessuno inizierà mai a usarlo, perché è un sistema che non si può introdurre un po' alla volta. È un circolo vizioso: se non vale la pena usarlo finché non è diffuso, allora nessuno inizierà a usarlo.

In ultima battuta, esso richiede collaborazione da parte di banche e utenti finali, cioè di attori estranei a quel popolo di Internet costituito da provider e amministratori di sistemi che, come detto, sanno cooperare agilmente in caso di necessità.

### **7.4.3. Tag per invii di massa**

Una possibile soluzione a lungo termine consiste nella definizione di marchi (tag) che descrivono come sono stati spediti i messaggi di massa. Questi tag vanno codificati in un protocollo che permetta ai server e-mail di indicare che tipo di messaggi accettano. Tale soluzione richiede nuovi programmi di posta sia lato client che server e va integrata con soluzioni a breve termine, ma è difficile da introdurre: si è visto come la modifica di protocolli ampiamente diffusi non sia né semplice né immediata. Personalmente ritengo poco probabile l'adozione di questo metodo, ma esso ha un vantaggio notevole: se si vuole intervenire legalmente sullo spamming, può essere la base legale per evitare di ricorrere a leggi fatte per altri scopi (privacy o abuso di infrastrutture di terzi) oppure di crearne di peggiori cercando di marchiare i messaggi di massa in base al contenuto (con tag come ADV nel soggetto). In pratica

si offre un sistema funzionante, che permette invii di massa in modo legale e legittimo. Se si compiono abusi si cade nel torto legale. Non è molto diverso da ciò che si sta già cercando di fare, ma questo sistema ha il vantaggio di agire in modo ufficiale con dei protocolli definiti. È un metodo poco intrusivo che forse vale la pena di sperimentare prima di passare a qualcosa di più deciso.

Gli attributi proposti per marciare i messaggi sono il numero di destinatari per messaggio e il tipo di relazione mittente-destinatario. I tag devono essere inclusi anche nell'header per consentire il passaggio attraverso diversi server e-mail. Infatti è possibile che il server e-mail che per primo riceve il messaggio non conosca le policy del server di destinazione.

Il tag proposto è di questo tipo:

```
Bulk-Tags: Recipients=300 By=stranger
```

I programmi di posta (server e client) filtreranno la posta con certi attributi, eventualmente distribuendola in diverse mailbox secondo il tipo.

Questi tag sono la base per un protocollo opt-out: è l'equivalente di mettere sul server e-mail l'adesivo "Niente pubblicità per favore". In pratica, si estende il protocollo SMTP in modo che il destinatario possa esprimere i suoi desideri prima ancora che i messaggi gli siano recapitati.

Ma come è possibile fare in modo che gli spammer, che molto spesso già ora abusano dove possono, adottino questo sistema? Incredibilmente, molti spammer sarebbero felici di aderire. Alcuni, per ottenere rispetto, hanno proposto un sistema simile perché vogliono che gli invii di massa siano un business serio.

Il momento in cui tutta la gente metterà un tag che identifichi la normale posta privata su tutti i messaggi, questo sistema avrà successo. Per far ciò i client di posta dovrebbero essere programmati per farlo automaticamente. Solo i programmi di posta di massa dovranno preoccuparsi di inserire il tag corretto.

Il tag "bulk" potrebbe essere sottoposto a regole di trademark in stile TRUSTe, in modo che il suo uso imponga di aderire a una certa etica. Il tag verrebbe poi concesso su licenza a chi è d'accordo di seguire certe regole. Chi lo usa senza licenza o infrange le regole diventa perseguibile legalmente per frode.

Il tag che conta i destinatari deve considerare il numero totale per tutta la vita del messaggio: se un messaggio viene inviato oggi a 100 destinatari e tra una settimana a 1000, il tag dovrà riportare come numero totale 1100. Si tratta di una stima che riguarda un fatto. Se qualcuno cerca qualche scappatoia (per esempio, alterando leggermente il messaggio in modo da crearne due diversi), potrebbe trovarsi costretto a difendere tale scelta davanti a una corte.

La parte del tag che descrive le relazioni, invece, ha quattro possibili valori: By Known (il mittente è conosciuto dal destinatario personalmente e attivamente, non basta che il mittente sia famoso), By Stranger (il destinatario non conosce il mittente), Solicited (il destinatario ha richiesto il messaggio), Simple (usato da utenti normali che non fanno invii di massa e quindi, per questo tipo di messaggi, la relazione non è importante).

Il filtro può essere configurato come si desidera: per esempio, si può desiderare di ricevere la posta da sconosciuti, ma solo se i destinatari sono meno di un numero definito, per esempio 50. In linea di massima, sono gli utenti a stabilire le policy individualmente, ma chi amministra un server e-mail può definirne di globali. L'importante è che queste siano dichiarate quando qualcuno tenta di inviare la posta con quel server e-mail.

Il server del mittente si servirà dei tag per comunicare con il server del destinatario sfruttando la riga RCPT TO:

```
RCPT TO: user@site.domain Recipients=40 By=stranger
```

Il server e-mail del destinatario potrà rispondere OK oppure inviare un codice speciale per rifiutarlo in base alle policy. In questo caso, il server mittente assumerà che la policy valga per un certo periodo (per esempio sei mesi) e ne terrà conto per futuri invii.

Questo sistema non allevia immediatamente il superlavoro dei server e-mail, ma a lungo termine porterebbe a un calo dello spamming indiscriminato. Esso sembra legittimare gli invii di massa, e in effetti è esattamente quello che fa: legittima gli invii di massa che rispondono a certe regole. Se qualcuno bara, è comunque possibile far capo agli altri sistemi (anche quelli a breve termine), e si può sempre provare a ricorrere alla legge.

#### **7.4.4. Riconoscere la massa**

Come quello appena esposto, quest'ultimo metodo proposto da Templeton non fornisce uno strumento diretto contro lo spamming. Infatti, quello che esporrò in questo sottocapitolo può servire come strumento per identificare (e sostenere anche di fronte a una corte giudiziaria) in modo inequivocabile un messaggio di massa. In particolare, lo scopo di questo strumento è di identificare in modo automatico un messaggio inviato a una massa di indirizzi, nonostante il destinatario ne riceva un solo esemplare.

Innanzitutto, è necessario definire la massa (bulk) nell'ambito del fenomeno dello spamming. Nella definizione che ho deciso di utilizzare per questa memoria, essa viene descritta come l'insieme di messaggi, aventi sostanzialmente lo stesso contenuto, a cui appartiene il messaggio di spam ricevuto.

L'insieme, o la massa, di messaggi va inteso come frutto di un automatismo per mandare lo stesso messaggio a molti destinatari che non sono in relazione fra loro. L'automatismo è l'uso di un computer per facilitare l'invio di uno stesso messaggio a molti indirizzi. Non si intende soltanto una lista di indirizzi o un programma di invio apposito: anche un programma che personalizza una lettera modello (per esempio inserendo un nome o un codice diverso su ogni esemplare) oppure uno che genera una lettera diversa dallo stesso contenuto sono automatismi. I destinatari che non sono in relazione tra loro sono persone che non si conoscono. Templeton propone che le copie necessarie per identificare una massa siano 25.

Gli essere umani riconoscono facilmente e senza (quasi) mai sbagliare un messaggio di massa, anche se esso è stato truccato per apparire personale, ma chi lo riceve non può provare che esso è di massa perché è in possesso di un'unica copia. La maggior parte dei messaggi di massa può essere riconosciuta anche da un software, perché le modifiche per mascherarli da messaggi personali sono minime nelle differenti copie. Ricevendo un unico esemplare, però, il software non può paragonare diverse copie e decidere se sono parte dell'insieme di messaggi aventi sostanzialmente lo stesso contenuto.

Naturalmente, i provider, soprattutto quelli di grosse dimensioni, possono riconoscere automaticamente la posta di massa senza coinvolgere i loro utenti. Per far ciò, possono usare una tecnica che genera l'hash<sup>48</sup> del messaggio (o di un paragrafo, o di una frase) e conservarlo in una banca dati. Quando un messaggio di massa arriva una seconda volta, esso può essere riconosciuto rapidamente anche se è stato manipolato per sfuggire proprio a questo tipo di tecniche. Se due messaggi hanno anche un solo paragrafo identico è molto probabile che siano in relazione. Questo in passato è stato fatto, ma le conseguenze sono state negative: AOL ha cancellato migliaia di lettere che la scuola di Harvard aveva inviato ad altrettanti utenti AOL per confermare l'ammissione ai corsi. Il computer non è in grado di distinguere un invio di massa sollecitato da uno non sollecitato.

È in atto una battaglia tra programmi che mascherano messaggi di massa, personalizzandoli, e programmi che tentano di individuare tali messaggi, ma alcune cose semplicemente non possono essere evitate: i messaggi di pubblicità per un prodotto o un'azienda devono contenere i nomi del prodotto o dell'azienda, che probabilmente saranno unici e coperti da trademark. Saranno inoltre presenti informazioni di contatto (numeri di telefono, indirizzi stradali o di pagine web) che sono facili da individuare anche in messaggi che in altre parti sono diversi. Inoltre, tutti i messaggi includono una traccia della strada che hanno percorso dal loro punto

---

<sup>48</sup> L'hash è una sorta di impronta digitale di un testo. Esso è statisticamente unico per ogni testo, ma dall'hash non è possibile risalire al testo d'origine.

d'origine. Per aiutare i provider di piccole dimensioni, i risultati del calcolo degli hash possono essere automaticamente distribuiti per la Rete.

Il sistema può essere perfezionato. Si possono creare falsi indirizzi da usare come trappole, sparpagliandoli per la Rete. In questo modo si possono raccogliere molti messaggi di spam e paragonarli tra loro. Il fatto che un messaggio arrivi a due di questi indirizzi trappola costituisce una prova solida che esso è parte di un invio di massa ed è stato spedito a uno sconosciuto.

Per individuare la posta di massa, si potrebbe creare un deposito centrale in modo che gli utenti possano verificare se un messaggio che hanno ricevuto è un messaggio di massa. Servirebbe semplicemente un indirizzo a cui inoltrare i messaggi sospetti. Il responso del sistema può essere un utile strumento se si vuole intentare una causa legale contro lo spammer o semplicemente protestare presso il suo provider: statisticamente è semplice provare che un messaggio praticamente identico arrivato a poche persone che non si conoscono in realtà è arrivato a molte persone. Inoltre, una volta che i messaggi di massa sono stati individuati, è possibile mettere la loro firma hash nelle liste di filtraggio, così che messaggi simili possano essere fermati prima che arrivino.

## 8. Test in rete

Per arricchire la memoria di licenza con una parte originale ho condotto alcuni test reali. Di qualcuno ho già parlato, ma in questo capitolo vengono presentati i risultati dei test più importanti. Si tratta di prove effettuate per sperimentare in prima persona ciò che ho trovato sui numerosi articoli e siti consultati durante la stesura di questo lavoro. Tengo a sottolineare che non hanno una valenza rappresentativa perché i messaggi analizzati sono troppo pochi rispetto a quelli in circolazione.

L'idea alla base di questi test è quella di capire quanti messaggi di spam si ricevono in relazione al modo in cui un certo indirizzo di posta elettronica viene reso pubblico. Per tentare di soddisfare queste curiosità bisogna cercare di ricevere spam. Per far ciò ho approfittato della collaborazione di Mario Gay, responsabile di TI-EDU, la rete per l'insegnamento superiore e di ricerca scientifica nella Svizzera italiana. In concreto, oltre ai preziosi consigli e suggerimenti, ho avuto la possibilità di utilizzare trenta indirizzi di posta elettronica, corrispondenti ad altrettante mailbox, creati appositamente sul server e-mail *posta.ti-edu.ch*.

I trenta indirizzi sono:

- da *ml01@ml.ti-edu.ch* a *ml15@ml.ti-edu.ch*;
- da *mlc01@cherou.com* a *mlc15@cherou.com*.

Questi indirizzi sono stati resi pubblici in vari modi, con lo scopo di attirare spam. Il modo più efficace si è rivelato, prevedibilmente, la pubblicazione su gruppi di discussione Usenet. Ma non sono stati trascurati altri mezzi. Sono state scelte tre famiglie di mezzi di pubblicazione: l'iscrizione a newsletter (affidabili e "losche"); la pubblicazione su diversi gruppi di discussione Usenet (newsgroup) e su una pagina web.

### 8.1. Newsletter

#### 8.1.1. Scopo del test e iscrizione alle newsletter

Una newsletter è un messaggio pubblicitario o d'informazione inviato periodicamente da un sito d'informazione o da un'azienda a chi ha indicato di volerla ricevere, fornendo il proprio indirizzo e-mail. Chi gestisce una newsletter ha quindi un archivio di molti indirizzi e-mail che sicuramente fa gola a molti spammer, i quali potrebbero offrirsi di acquistarlo (oppure potrebbero rubarlo, se l'archivio non è adeguatamente protetto).

Lo scopo di questo test è quello di verificare se l'iscrizione a una newsletter comporta il rischio di ricevere spam. Ho cercato quattro newsletter con diversi livelli di affidabilità basati sulla fiducia "ispirata" da fattori oggettivi e soggettivi. Gli indirizzi usati per l'iscrizione non sono stati utilizzati o resi pubblici in alcun altro modo. Per verificare se vi sono differenze di trattamento a dipendenza del tipo di indirizzo iscritto, per ogni newsletter sono stati usati due indirizzi: uno del dominio svizzero *ti-edu.ch* e uno del dominio internazionale *cherou.com*.

La newsletter che ho considerato più affidabile è quella di **Verisign** (ora è tornata a chiamarsi Network Solutions), perché sulla pagina dell'iscrizione è presente il logo TRUSTe. Significa quindi che ci sono delle Privacy Policy approvate e garantite da una terza parte.

A livello intermedio ho considerato le newsletter di Coffeecup e Buongiorno.it. **Coffeecup** è un'azienda che produce software per il web. L'ho considerata affidabile per due motivi: il primo è che ha delle Privacy Policy in cui viene affermato con forza che l'indirizzo non sarà usato per spam né venduto. Il secondo motivo è che mi ero precedentemente iscritto con un altro indirizzo e avevo ricevuto, il 12 settembre 2001, un messaggio molto emotivo e patriottico del CEO dell'azienda, in cui si commentavano gli attentati del giorno precedente. La presenza personale sulla newsletter del CEO di un'azienda attiva nel mercato del web mi ha ispirato fiducia. Nonostante ciò non ha il marchio TRUSTe. **Buongiorno.it** è un servizio gratuito specializzato in newsletter. Ne esistono centinaia dagli argomenti più diversi. Un tempo ci sono state polemiche sul modo in cui veniva gestito: era molto semplice iscrivere qualunque indirizzo, senza necessità di conferma, a decine di newsletter.

**Meridianlaunch** è la newsletter di un'azienda pubblicizzata sul newsgroup *alt.alcohol*, per questo l'ho considerata inaffidabile. Il sito ha cambiato gestione durante il test, oggi riporta delle Privacy Policy e la pagina di iscrizione non esiste più.

L'iscrizione alle newsletter è avvenuta il 19 novembre 2001, tranne per quella di Meridianlaunch, che ha avuto luogo il 14 dicembre 2001.

### 8.1.2. Risultati e commento

Il 18 novembre 2002, quindi dopo un anno, la situazione era quella descritta nella tabella che segue. Nella prima colonna si trova l'indirizzo usato per l'iscrizione alla newsletter, il cui mittente viene indicato nella seconda colonna. Nella terza colonna è indicata la quantità di messaggi ricevuti nell'anno di osservazione e nella quarta quella di spam ricevuto.

Indirizzo iscritto alla newsletter	Mittente della newsletter	# messaggi ricevuti in totale	# messaggi di spam ricevuti
ml01@ml.ti-edu.ch	Coffeecup	15 messaggi	0 messaggi
mlc01@cherou.com	Coffeecup	15 messaggi	0 messaggi
ml02@ml.ti-edu.ch	Buongiorno.it	389 messaggi	0 messaggi
mlc02@cherou.com	Buongiorno.it	387 messaggi	0 messaggi
ml03@ml.ti-edu.ch	Verisign	1 messaggio	0 messaggi
mlc03@cherou.com	Verisign	1 messaggio	0 messaggi
ml08@ml.ti-edu.ch	Meridianlaunch	1 messaggio	0 messaggi
mlc08@cherou.com	Meridianlaunch	1 messaggio	0 messaggi

Tabella 3: newsletter, situazione dopo un anno

Da **Verisign** è arrivato su ciascun indirizzo iscritto un solo messaggio, che richiedeva la conferma dell'iscrizione tramite la visita a una pagina web. Conferma che è stata data a più riprese nei giorni successivi, ma che evidentemente non ha funzionato. Ho fatto altri tentativi, ma senza successo. A parte questo problema, non è arrivato alcun messaggio di spam.

**Coffeecup** ha usato l'indirizzo correttamente per pubblicizzare i suoi prodotti, senza cederlo a terzi. Non è arrivato alcun messaggio di spam e non si notano differenze tra i due indirizzi iscritti.

**Buongiorno.it** ha inviato i messaggi richiesti, uno al giorno, sui due indirizzi e non è arrivato spam. Il 19 novembre 2002, esattamente un anno dopo l'iscrizione, ho provveduto a rimuovere i due indirizzi dalla newsletter alla quale li avevo abbonati. Immediatamente l'invio dei messaggi è cessato. Sono arrivati anche messaggi di pubblicità di nuovi servizi, che sembrano mandati periodicamente ad alcuni iscritti, presumibilmente a rotazione. Per questo si nota la differenza di due messaggi tra i due indirizzi. Il 13 dicembre 2002, quasi un mese dopo la rimozione dell'iscrizione, a entrambi gli indirizzi è arrivato un messaggio pubblicitario sui prodotti di Buongiorno.it. Il trucco è questo: iscrivendosi a una delle newsletter si accetta di ricevere anche i messaggi pubblicitari. Rimuovendo l'iscrizione dalla newsletter, si rimane "abbonati" ai messaggi pubblicitari, per i quali è necessari un'altra procedura. I messaggi pubblicitari arrivati in quest'anno sono stati comunque solo una ventina in totale.

Anche nel caso di **Meridianlaunch** è arrivato unicamente un messaggio che richiedeva di visitare una pagina web per confermare l'iscrizione. La conferma è stata data, ma non sono arrivati altri messaggi. Come anticipato, il sito è cambiato. Da qualche informazione raccolta in rete, sembra che qualche loro (ex) rivenditore abbia distribuito spam su Usenet. L'azienda pare comunque seria, anche perché non è arrivato alcun messaggio di spam.

Nel complesso sembra che l'iscrizione a qualche newsletter non comporti il rischio di ricevere messaggi di spam.

## 8.2. Usenet e web

### 8.2.1. Scopo del test

Questo secondo test è destinato soprattutto a osservare quanto spam si riceve a seconda di come si rende pubblico un indirizzo. In particolare ho considerato la tendenza nella ricezione di messaggi di spam per indirizzi pubblicati su diversi newsgroup e su una pagina web. Come vedremo, il confronto con la pubblicazione su web non è stato possibile.

Inoltre ho utilizzato questa prova per verificare se un indirizzo in un dominio svizzero istituzionale (*ti-edu.ch*) venga trattato dagli spammer diversamente da un indirizzo in un dominio internazionale (*cherou.com*). Un trattamento diverso potrebbe indicare una certa attenzione all'orientamento del mercato.

### 8.2.2. Pubblicazione degli indirizzi

Ogni indirizzo è stato pubblicato sul newsgroup mandando un unico messaggio avente come mittente l'indirizzo in questione. Nessun indirizzo è stato usato in altro modo. Ho inviato messaggi dal contenuto verosimile, anche se presumo che esso sia irrilevante ai fini di test di questo tipo.

Nella tabella seguente viene indicato nella prima colonna l'indirizzo pubblicato e, nella seconda, il luogo dove è stato pubblicato. La terza colonna riporta la data di pubblicazione. Come si può notare, il 19 novembre 2001 è avvenuta la pubblicazione su quattro newsgroup mentre il 13 giugno 2002 essa è stata ripetuta ed è stata effettuata anche la pubblicazione sulla pagina web.

Indirizzo pubblicato	Luogo di pubblicazione	Data di pubblicazione
ml04@ml.ti-edu.ch	ch.comp.os.linux (newsgroup)	19 novembre 2001
mlc04@cherou.com	ch.comp.os.linux (newsgroup)	19 novembre 2001
ml05@ml.ti-edu.ch	comp.mail.pine (newsgroup)	19 novembre 2001
mlc05@cherou.com	comp.mail.pine (newsgroup)	19 novembre 2001
ml06@ml.ti-edu.ch	it.hobby.cucina (newsgroup)	19 novembre 2001
mlc06@cherou.com	it.hobby.cucina (newsgroup)	19 novembre 2001
ml07@ml.ti-edu.ch	alt.alcohol (newsgroup)	19 novembre 2001
mlc07@cherou.com	alt.alcohol (newsgroup)	19 novembre 2001
ml10@ml.ti-edu.ch	ti-edu (web in chiaro)	13 giugno 2002
mlc10@cherou.com	ti-edu (web in chiaro)	13 giugno 2002
ml11@ml.ti-edu.ch	ti-edu (web con script)	13 giugno 2002
mlc11@cherou.com	ti-edu (web con script)	13 giugno 2002
ml12@ml.ti-edu.ch	ch.comp.os.linux (newsgroup)	13 giugno 2002

mlc12@cherou.com	ch.comp.os.linux (newsgroup)	13 giugno 2002
ml13@ml.ti-edu.ch	comp.mail.pine (newsgroup)	13 giugno 2002
mlc13@cherou.com	comp.mail.pine (newsgroup)	13 giugno 2002
ml14@ml.ti-edu.ch	it.hobby.cucina (newsgroup)	13 giugno 2002
mlc14@cherou.com	it.hobby.cucina (newsgroup)	13 giugno 2002
ml15@ml.ti-edu.ch	alt.alcohol (newsgroup)	13 giugno 2002

Tabella 4: Usenet e web, pubblicazione degli indirizzi

I quattro gruppi di discussione sono *ch.comp.os.linux* (gruppo della gerarchia svizzera, in tedesco, dedicato a Linux); *comp.mail.pine* (gruppo internazionale, in inglese, dedicato al programma di posta Pine); *it.hobby.cucina* (gruppo italiano dedicato alla cucina); *alt.alcohol* (gruppo della gerarchia alternativa dedicato all'alcol). Quest'ultimo gruppo è da considerare pericoloso, nel senso che il poco traffico che ha è spam. La gerarchia *alt.\** viene rifiutata da alcuni provider perché la sua gestione è troppo caotica e a volte causa problemi sui server. La pubblicazione su tutti i gruppi di discussione è avvenuta da un PC dell'Università della Svizzera Italiana, utilizzando il server news *news.cscs.ch* e il programma di posta elettronica e news PC-Pine (v 4.x).

L'indirizzo della pagina web è <http://www.ti-edu.ch/servizi/informatica/tesi-fare.html> ed è presente un link sulla pagina principale del sito (<http://www.ti-edu.ch/>). Il link è visibile solo osservando il codice HTML della pagina. In questo modo non dà fastidio ma è visibile dai software automatici. Due indirizzi sono stati pubblicati in chiaro, cioè con il tradizionale link, mentre per altri due ho sfruttato lo script riportato nel capitolo 7.2.2. Per dare ancor più visibilità alla pagina, visto che i risultati si facevano attendere, ho postato l'indirizzo della stessa su *it.test* il 12 settembre 2002.

### 8.2.3. Preparazione dell'analisi

L'estrazione dei messaggi dalle mailbox e il loro inserimento nella banca dati ha richiesto un lavoro impegnativo, pertanto è stata effettuata soltanto una volta, il 18 novembre 2002, e non più ripetuta. Nonostante ciò, le mailbox sono rimaste attive e, in alcuni casi, ho verificato come le cose erano procedute anche dopo il 18 novembre 2002 (comunque solo fino al 9 gennaio 2003).

Per analizzare i messaggi li ho trasferiti dalle mailbox in una banca dati, con il quale è stato possibile realizzare le query SQL per costruire le analisi e i grafici. Il trasferimento ha richiesto numerosi tentativi prima di riuscire ad avere i dati in una forma adeguata. In questa parte sono stato aiutato da Davide Airaghi, supervisionato da Maurizio Cavalletti, entrambi della Sertel srl di Milano, il cui amministratore delegato è il dottor Paolo Simonotti che conosco personalmente. Il personale della Sertel ha realizzato uno script che ha automatizzato il processo

di estrazione e generazione della banca dati, utile in particolare per la parte relativa alle date dei messaggi: il campo Date è spesso errato, per cui l'unico modo per conoscere realmente la data di arrivo di un messaggio è guardare quella inserita nei campi Received dall'ultimo server di posta attraversato (*posta.ti-edu.ch* nel nostro caso).

Ho incontrato alcuni problemi di ordine tecnico. Molti messaggi di spam, per esempio, non sono corretti formalmente (abbiamo trovato un campo To con 16.000 caratteri). Questo non mi ha permesso di utilizzare lo script per tutte le mailbox: per alcune l'esecuzione del programma si bloccava, perciò ho usato un prodotto creato appositamente per leggere le mailbox e generare le banche dati. Si chiama Email2FMP ed è stato realizzato da un'azienda informatica di Los Angeles (Adberg Consulting LCC<sup>1</sup>).

Il procedimento con Email2FMP è stato il seguente:

- lettura della mailbox tramite Eudora e archiviazione dei messaggi su file locale;
- estrazione, con Email2FMP, dal file di Eudora e generazione di una banca dati FilemakerPro;
- conversione della banca dati dal formato FilemakerPro al formato DBF (possibile solo grazie alla versione completa di Email2FMP) e importazione in Access;
- confronto manuale tra il campo Date e l'ultima riga del campo Received.

Una volta ottenuto un unico file leggibile da Access ho scritto le query SQL e infine ho analizzato i dati con un foglio elettronico (sono stati usati sia OpenOffice che Excel).

A parte qualche messaggio di test inviato dal mio indirizzo all'università alle mailbox presso TI-EDU, non sono arrivati altri messaggi. Quindi, nei conteggi sono stati considerati solo i messaggi di spam ricevuti.

Grazie alle query SQL ho contato i messaggi ricevuti in un arco di tempo compreso tra due date. Per il conteggio totale ho utilizzato l'intervallo tra il 19 novembre 2001 e il 18 novembre 2002. Per realizzare i grafici ho scelto intervalli di un mese (tra il giorno 19 e il giorno 18 del mese successivo).

Nell'esempio che segue riporto la query utilizzata per contare i messaggi ricevuti sull'indirizzo *ml04@ml.ti-edu.ch* tra il 19 novembre 2001 e il 18 dicembre 2001 (che nei grafici verrà indicato come nov/dic):

```
SELECT *
FROM tab_msg
WHERE (date>#11/18/01# AND date<#12/19/01#) AND
folder="ml04";
```

---

<sup>1</sup> **Adberg Consulting LCC**, <http://www.adbergllc.com/>. La pagina dedicata a Email2FMP si trova presso <http://www.adbergllc.com/email2fmp.html>.

Ottenuta una tabella con i valori numerici per mailbox e per mese, ho potuto ricavare la visualizzazione grafica dell'andamento della ricezione dei messaggi di spam.

#### 8.2.4. Risultati

Tutti i risultati si riferiscono al 18 novembre 2002, cioè un anno dopo l'apertura dei primi test. Vediamo subito i risultati globali:

Indirizzo pubblicato	Luogo di pubblicazione	# messaggi di spam ricevuti
ml04@ml.ti-edu.ch	ch.comp.os.linux (newsgroup)	155
mlc04@cherou.com	ch.comp.os.linux (newsgroup)	110
ml05@ml.ti-edu.ch	comp.mail.pine (newsgroup)	93
mlc05@cherou.com	comp.mail.pine (newsgroup)	77
ml06@ml.ti-edu.ch	it.hobby.cucina (newsgroup)	84
mlc06@cherou.com	it.hobby.cucina (newsgroup)	59
ml07@ml.ti-edu.ch	alt.alcohol (newsgroup)	104
mlc07@cherou.com	alt.alcohol (newsgroup)	126
ml10@ml.ti-edu.ch	ti-edu (web in chiaro)	4
mlc10@cherou.com	ti-edu (web in chiaro)	0
ml11@ml.ti-edu.ch	ti-edu (web con script)	0
mlc11@cherou.com	ti-edu (web con script)	0
ml12@ml.ti-edu.ch	ch.comp.os.linux (newsgroup)	18
mlc12@cherou.com	ch.comp.os.linux (newsgroup)	14
ml13@ml.ti-edu.ch	comp.mail.pine (newsgroup)	32
mlc13@cherou.com	comp.mail.pine (newsgroup)	29
ml14@ml.ti-edu.ch	it.hobby.cucina (newsgroup)	8
mlc14@cherou.com	it.hobby.cucina (newsgroup)	11
ml15@ml.ti-edu.ch	alt.alcohol (newsgroup)	31
mlc15@cherou.com	ch.comp.os.linux (newsgroup)	42

Tabella 5: Usenet e web, risultati globali al 19 novembre 2002

Si nota subito che la pubblicazione sulla pagina web ha fornito risultati di difficile interpretazione: sono arrivati troppo pochi messaggi. Per questa ragione nei grafici non ho considerato le mailbox pubblicate su web.

Posso solo ipotizzare la causa dell'arrivo di così pochi messaggi. Probabilmente il sito di TI-EDU, pur essendo attivo da anni, non è molto noto al di fuori di una cerchia di siti perlopiù accademici. Gli indirizzi, inoltre, non sono stati messi sulla prima pagina, ma in una pagina creata ad hoc, per quanto la stessa era linkata nella prima pagina. Inoltre, probabilmente, gli spammer non sfruttano le pagine web come primaria fonte di indirizzi.

Qualche osservazione però ha senso. Qualcuno effettivamente ha esplorato le pagine trovando uno dei due indirizzi in chiaro. Uno di questi quattro messaggi è arrivato prima della pubblicazione dell'indirizzo della pagina web sul newsgroup *it.test*. Non so spiegare come mai gli stessi mittenti non abbiano usato anche l'altro indirizzo pubblicato in chiaro per i loro invii di spam. Forse cercavano solo indirizzi svizzeri.

Vale la pena indagare di più sulla natura dei quattro messaggi ricevuti: alcune somiglianze mi hanno portato a verificare che su quattro due arrivano dallo stesso mittente e pubblicizzano in lingua inglese un servizio di directory per il sito *www.ti-edu.ch*. Un altro è probabilmente imparentato mentre l'ultimo è diverso e promuove un sito pornografico tedesco a pagamento.

Il 9 gennaio 2003 ho controllato ancora le mailbox. Su *ml10@ml.ti-edu.ch* ho trovato altri quattro messaggi, tre dello stesso mittente dei servizi di directory e uno in lingua italiana che pubblicizza un'agenzia immobiliare di Varese. L'ingenuità del messaggio (firmato con il nome dell'azienda, indirizzo stradale, numero di telefono e nome e cognome del titolare) contrasta con la probabile modalità con cui l'indirizzo è stato raccolto. Questo messaggio, inoltre, è arrivato anche su *mlc10@cherou.com*, l'altro indirizzo pubblicato in chiaro.

Sugli indirizzi pubblicati con lo script non è arrivato nulla (nemmeno dopo il controllo del 9 gennaio 2003). Non mi sento di concludere che lo script effettivamente protegge l'indirizzo perché i messaggi arrivati sugli indirizzi pubblicati in chiaro sono troppo pochi. Però la tendenza sembra essere proprio questa.

### **8.2.5. Grafici dell'andamento**

I risultati sono presentati ora in forma grafica per evidenziare le tendenze. Cominciamo con i grafici relativi ai singoli gruppi di discussioni. Ogni grafico riporta l'andamento delle quattro caselle di posta pubblicate sullo stesso newsgroup. Gli indirizzi pubblicati il 13 giugno 2002 hanno ricevuto un minor numero di messaggi. Un confronto è tuttavia possibile osservando le curve e le tendenze.

Siccome i numeri sono relativamente piccoli, non bisogna considerare le differenze episodiche. Anche se su un grafico può apparire una grossa differenza, in realtà potrebbe trattarsi di cinque o dieci messaggi. Mi sono concentrato sull'osservazione delle tendenze, più che sull'effettivo numero di messaggi di spam ricevuti.

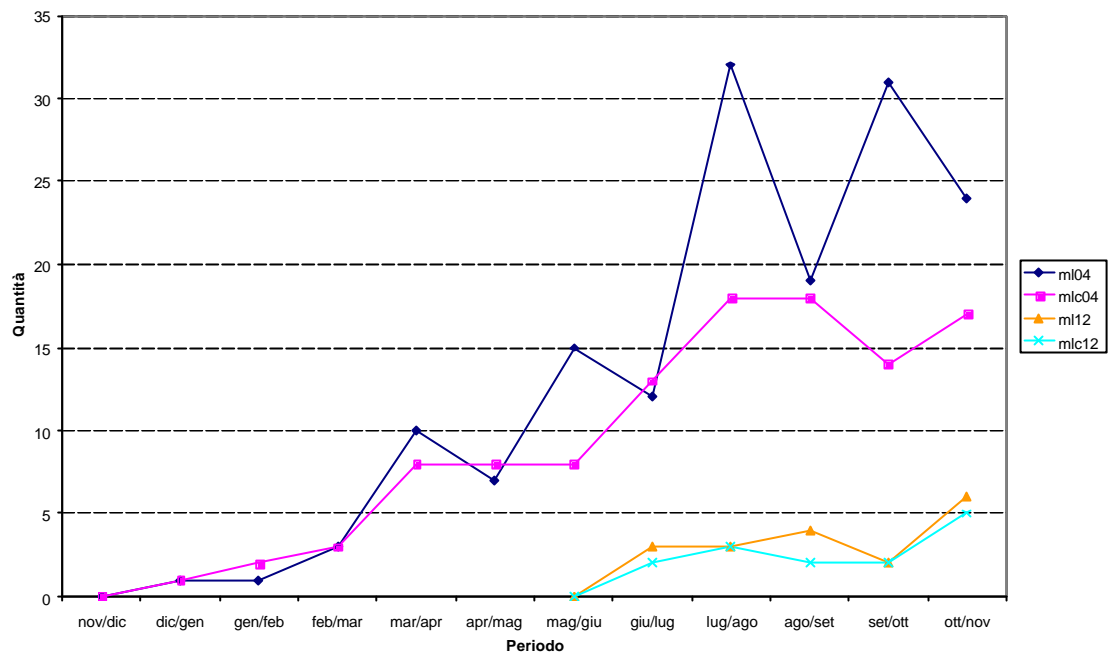


Figura 3: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su *ch.comp.os.linux*

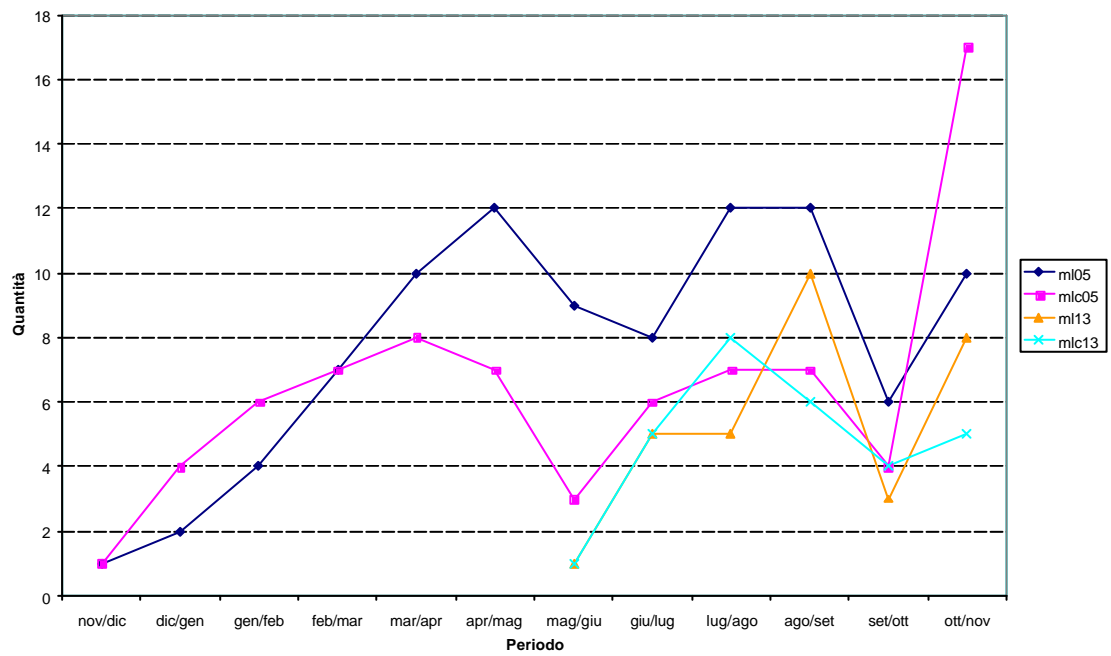


Figura 4: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su *comp.mail.pine*

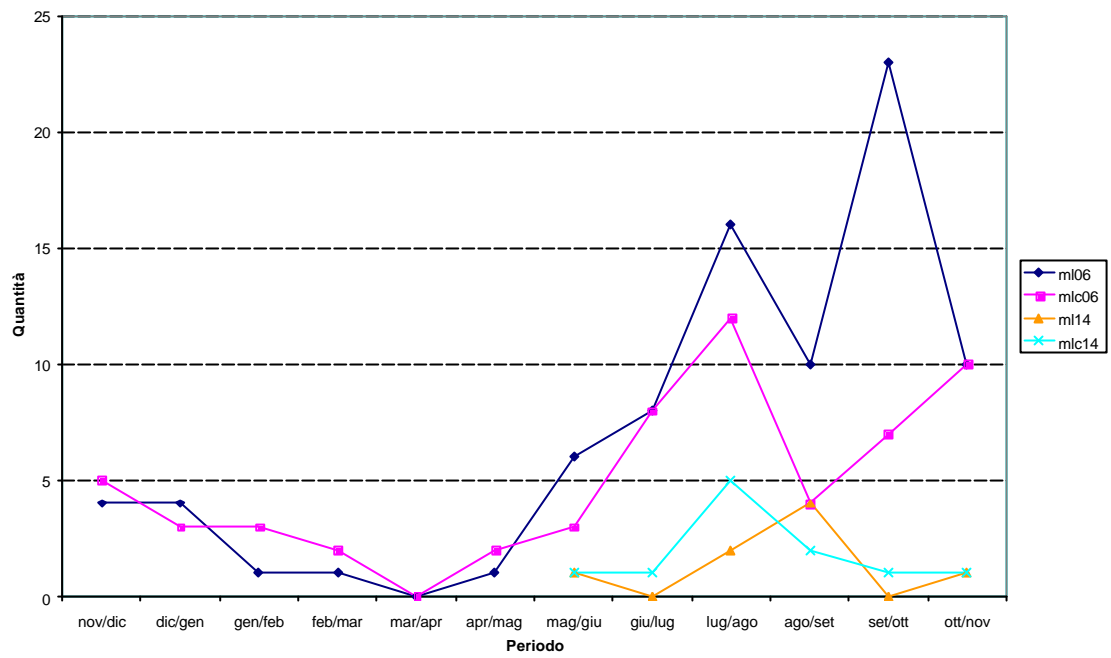


Figura 5: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su *it.hobby.cucina*

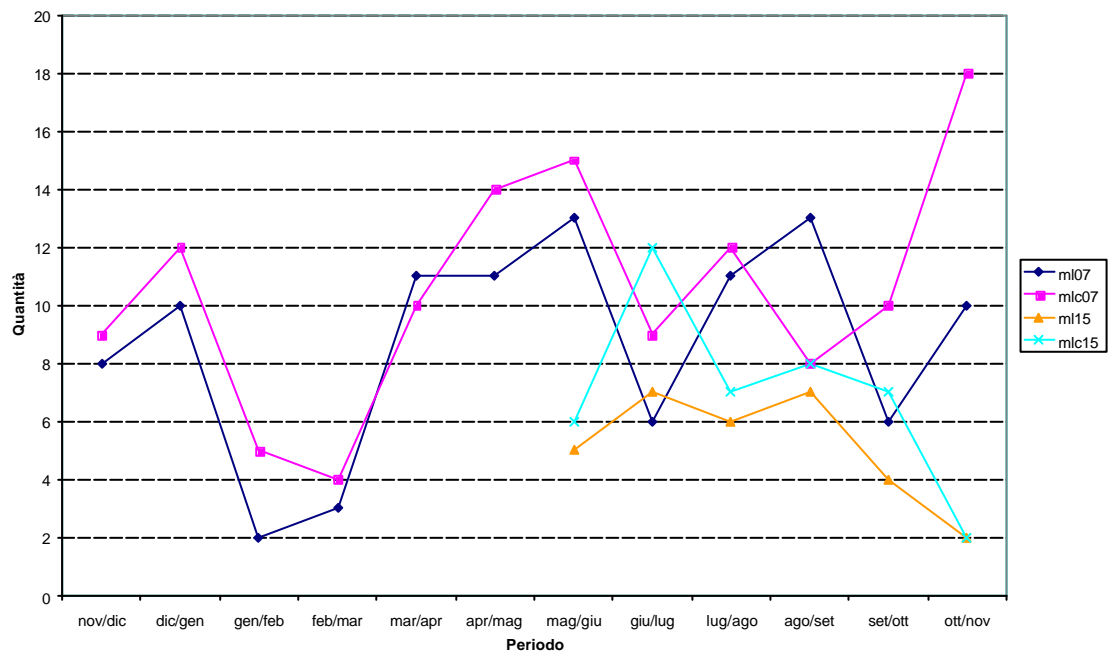


Figura 6: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su *alt.alcohol*

### 8.2.6. Commento

Si nota immediatamente come la tendenza generale sia quella dell'aumento del numero di messaggi di spam ricevuti. Questo sembra confermare quanto riportato dagli osservatori (Brightmail stima che lo spam in circolazione sia triplicato tra il novembre del 2001 e il novembre del 2002). In effetti, l'impressione generale che ricevo da tutte le altre mailbox di questo test e dalle mie private è la stessa, ma non mi sento di dare quest'interpretazione perché altri fattori portano a un aumento di spam su queste mailbox. Gli indirizzi, infatti, una volta pubblicati e inseriti nelle liste degli spammer, vengono venduti e rivenduti. Pertanto, dopo un anno, lo stesso indirizzo potrebbe essere finito in decine di liste diverse e questo, da solo, potrebbe giustificare l'aumento. Questa è anche la ragione per cui gli indirizzi pubblicati nel giugno del 2002 hanno ricevuto meno messaggi: semplicemente erano meno diffusi.

Nonostante i picchi di alcune mailbox si evidenzia una tendenza comune tra i diversi indirizzi pubblicati su uno stesso newsgroup: la crescita avviene più o meno negli stessi periodi. Gli indirizzi pubblicati in giugno hanno ricevuto troppo pochi messaggi per un confronto realmente affidabile, ma le curve sono comunque abbastanza simili tra di loro.

Vi è poca differenza tra le mailbox *ti-edu.ch* e quelle *cherou.com* per lo stesso newsgroup, anche se ci sono stati alcuni picchi effettivamente diversi. Presumibilmente gli spammer non si interessano a chi appartengono gli indirizzi che raccolgono. L'impressione è che il prezzo di un indirizzario sia determinato dalla quantità di indirizzi elencati, non dalla loro qualità.

Durante l'anno in cui le mailbox sono state attive pensavo di aver ricevuto pochi messaggi di spam. Temevo che questo fosse dovuto al fatto che gli indirizzi sono stati pubblicati nei newsgroup una sola volta, cosa che è anche abbastanza improbabile: chi frequenta i newsgroup, e scrive, non si limita a un solo messaggio all'anno ma normalmente è più attivo. La mailbox che ne ha ricevuti di più è stata *ml04@ml.ti-edu.ch*: 155 in un anno. Altre mailbox ne hanno ricevuti molti di più: alla casella su Hotmail ne sono arrivati più di mille in sette mesi. Ma, in seguito, ho notato che 155 messaggi in un anno non sono così pochi: i due indirizzi di posta che uso abitualmente, anche sui gruppi di discussione, hanno collezionato complessivamente circa 500 messaggi in due anni, che significa 125 messaggi per mailbox ogni anno.

### 8.2.7. Confronto tra i gruppi di discussione

Il grafico seguente mostra l'andamento dei messaggi di spam confrontando i quattro newsgroup dove sono stati pubblicati gli indirizzi. Per ogni newsgroup ho utilizzato la somma dei messaggi ricevuti in ogni mailbox pubblicata su quello stesso gruppo.

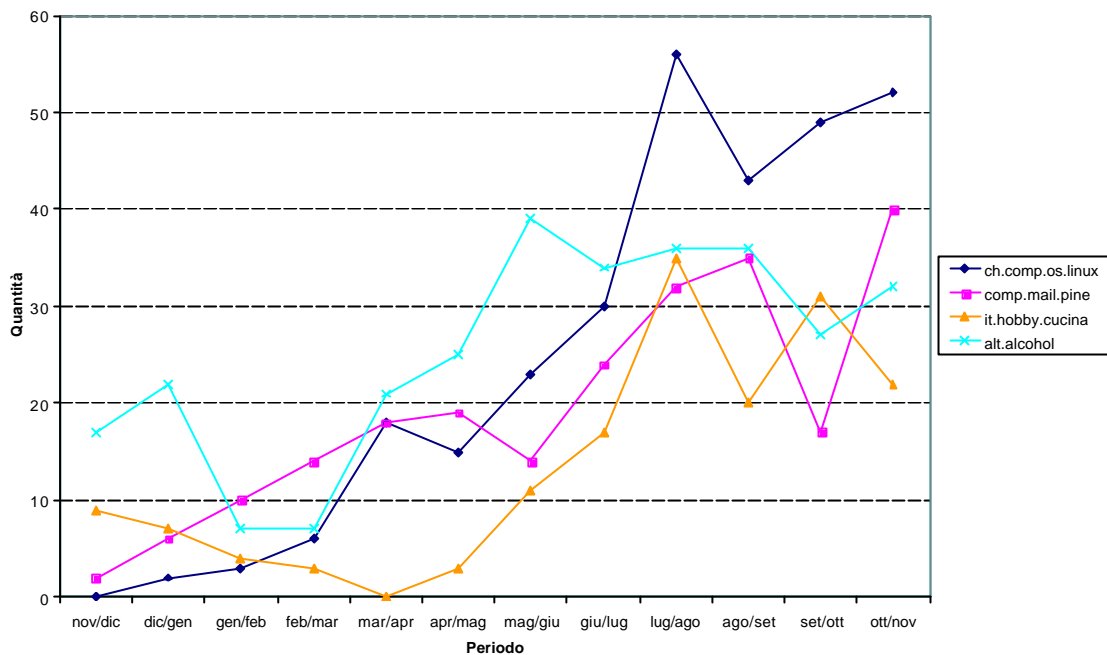


Figura 7: confronto tra i gruppi di discussione

Il trend globale, anche qui, è quello dell'aumento. Dato l'esiguo numero di messaggi ricevuti, è difficile fare paragoni che vadano oltre. Si possono notare alcuni periodi in cui la crescita è particolarmente evidente: in marzo la crescita dello spam ricevuto sugli indirizzi pubblicati su *ch.comp.os.linux* e su *alt.alcohol* è molto forte, mentre quello ricevuto dagli indirizzi pubblicati su *comp.mail.pine* cresce in modo costante e quello per gli indirizzi su *it.hobby.cucina* diminuisce. Approssimativamente tra maggio e agosto, invece, tutti gli indirizzi registrano un'impennata.

In sostanza non vedo differenze particolarmente significative nei trend dei quattro newsgroup.

### 8.3. Altri test

Presento un rapido riepilogo degli altri test effettuati.

#### 8.3.1. Confronto tra indirizzi

Questo test (anticipato nel capitolo 5.2.3.) sembra dimostrare che gli spammer usino generatori automatici per compilare le loro liste di indirizzi e-mail. Nessuno degli indirizzi è mai stato usato pubblicamente. Nella tabella seguente troviamo i risultati precisi del test.

Indirizzo	Data creazione	# messaggi di spam ricevuti	Controllato fino alla data	Data del primo spam ricevuto
<i>mfare@bluewin.ch</i>	14.01.2002	108	08.01.2003	16.08.2002
<i>a6.c-h2.n.h-u@bluewin.ch</i>	19.04.2002	0	08.01.2003	-
<i>mimi1080@hotmail.com</i>	11.06.2002	1353	08.01.2003	13.06.2002
<i>z9_u_b7_d_b_a@hotmail.com</i>	11.06.2002	0	08.01.2003	-
<i>mfare@freesurf.ch</i>	01.2002	55	08.01.2003	12.10.2002

Tabella 6: generazione automatica, confronto tra indirizzi

Si nota come gli indirizzi semplici (*mimi1080@hotmail.com*, *mfare@bluewin.ch* e *mfare@freesurf.ch*) siano stati oggetti di spamming, al contrario di quelli complessi (*a6.c-h2.n.h-u@bluewin.ch* e *z9\_u\_b7\_d\_b\_a@hotmail.com*). I conteggi di Hotmail escludono i messaggi di servizio (15 in totale per ogni indirizzo). Su *mimi1080@hotmail.com* i messaggi di spam sono arrivati quasi immediatamente (dopo due giorni dalla sua creazione). Su *mfare@freesurf.ch*, creato all'inizio del 2002, c'è voluto più tempo (alcuni mesi), così come su *mfare@bluewin.ch* (otto mesi).

Ho attribuito questa situazione alla possibilità di generare indirizzi in modo automatico. Tra le altre possibilità c'è naturalmente quella di penetrare nelle banche dati dei gestori di servizi di questo tipo e rubare, nel vero senso della parola, gli indirizzi. Le leggende dicono che uno spammer abbia forzato i sistemi di Hotmail e abbia sottratto centinaia di migliaia di indirizzi per mesi.

Per quanto riguarda i messaggi ricevuti su *mfare@bluewin.ch*, è da notare il fatto che ben 34 messaggi sono in tedesco e 26 in francese, e solo 48 sono in inglese. Sull'indirizzo *mfare@freesurf.ch* la situazione è ancora più evidente: 44 messaggi in tedesco e solo 11 in inglese.

Ecco la tabella riassuntiva:

<b>mfare@freesurf.ch</b>			<b>mfare@bluewin.ch</b>		
Lingua	Messaggi	Percentuale	Lingua	Messaggi	Percentuale
Tedesco	34	31.5%	Tedesco	44	80 %
Inglese	48	44.4%	Inglese	11	20 %
Francese	26	24.1%			
<b>Totali</b>	108	100%		55	100%

Tabella 7: lingua dei messaggi, confronto tra indirizzi

### 8.3.2. Filtro anti-spam per webmail

Dal capitolo 7.3.8. riporto i dati sull'uso del filtro anti-spam messo a disposizione da Hotmail:

I livelli sono tre:

- **Predefinito:** viene bloccata la posta palesemente indesiderata;
- **Alto:** viene bloccata la maggior parte della posta indesiderata;
- **Esclusivo:** vengono recapitati solo i messaggi da indirizzi presenti nei Contatti o nell'Elenco Posta protetta.

È stato scelto il filtro di livello "Alto". La posta bloccata è stata recapitata in un'apposita cartella. Il filtro è stato applicato all'indirizzo *mimi1080@hotmail.com* nel periodo tra il 14 agosto 2002 (data di attivazione del filtro) e l'8 gennaio 2003 (ultimo controllo).

Si nota come molto spam (più del 70%) sia passato, nonostante il filtro.

	Messaggi di spam ricevuti	Percentuale rispetto al totale
<b>Intercettati dal filtro</b>	252	28.25 %
<b>Sfuggiti al filtro</b>	636	71.75 %
<b>Spam ricevuti in totale</b>	892	100 %

Tabella 8: risultati filtri anti-spam

### 8.3.3. "Toglimi" nell'indirizzo mittente

Sono del capitolo 7.2.1., invece, i dati relativi all'uso di una stringa nell'indirizzo mittente. Un messaggio inviato a 14 persone con mittente *mfare@swissonline.toglimi.ch* invece di *mfare@swissonline.ch* ha ricevuto solo due risposte, da due persone che hanno dovuto compiere qualche tentativo per riuscire a replicare.

L'uso di tecniche per mascherare l'indirizzo reale dunque complica la normale comunicazione, ma ha il pregio di impedire anche l'arrivo di messaggi di spam: due messaggi, mandati il 21 ottobre 2002 al newsgroup *alt.alcohol*, con mittenti *ml09@ml.ti-edu.toglimi.ch* e *mlc09@cherou.toglimi.com* invece di *ml09@ml.ti-edu.ch* e *mlc09@cherou.com*, il 7 gennaio 2003 non avevano ancora causato l'arrivo di spam.

### 8.3.4. Indirizzario da Usenet

Una prova di un attivista anti-spam, raccontata nel capitolo 5.2.1., ha dimostrato che in poche ore si possono raccogliere molti indirizzi dai newsgroup. L'attivista è riuscito a raccogliere 124.322 indirizzi validi ricavati soltanto dai newsgroup italiani

## 8.4. Commenti finali

L'impressione generale ottenuta da tutti questi test è che gli spammer usino, per compilare i loro indirizzi, principalmente Usenet e la generazione automatica. Ipotizzo anche che siano molti i siti che, in un modo o nell'altro, raccolgono gli indirizzi e-mail di chi li visita. Questa ipotesi deriva dal fatto che i frequentatori di Usenet sono pochi, rispetto al totale dei navigatori in Internet, ma tutti ricevono spam. La raccolta da web può avvenire, come detto, attraverso la lettura dagli indirizzi su pagine web (soprattutto quelle dei forum), script in javascript o altri metodi invisibili. Penso che molti siti a contenuto "losco" (pornografia o casinò on-line, per esempio) siano responsabili di quest'azione, ma non mancano certamente newsletter fittizie, create con l'unico scopo di raccogliere indirizzi da rivendere.

## 9. Conclusione

La tecnologia è uno strumento, che può essere usato per fini pacifici oppure violenti: dipende da chi la usa, dipende dall'Uomo. Fortunatamente le tecnologie nel campo della comunicazione non hanno applicazioni fisicamente violente, ma possono comunque essere utilizzate per scopi inappropriati. Ogni nuova tecnologia della comunicazione apre un nuovo canale verso la nostra persona. L'evoluzione storica è sotto gli occhi di tutti: un tempo, per comunicare con qualcuno, era necessario andare di persona o mandare qualcuno con un messaggio. Questa seconda possibilità si è evoluta fino a diventare il sistema di posta cartacea in uso oggi. Il telefono ha creato un ulteriore canale di accesso, che porta la voce di chi desidera comunicare con noi all'interno delle nostre case, in qualsiasi momento. In tempi più recenti l'avvento della telefonia mobile ha sconvolto le nostre abitudini telefoniche, rendendo gran parte della popolazione raggiungibile sempre e ovunque. L'abuso di questi mezzi è una forma di intrusione nella nostra sfera privata, un piccolo atto violento che ci impone la sospensione della nostra attività e ci obbliga a dedicare un certo tempo (risorsa sempre più preziosa) a chi sta comunicando con noi.

Fino all'arrivo della posta elettronica i mezzi di comunicazione erano disponibili a pagamento. Sono arrivati gradualmente, introdotti da un'autorità più o meno centrale in grado di esercitare un certo controllo. Le regole della buona educazione, che si sono adattate ai nuovi mezzi introducendo una nuova cultura della comunicazione, hanno permesso di distinguere facilmente gli abusi dall'uso appropriato. Internet ha sconvolto un'altra volta l'evoluzione del mondo della comunicazione. È talmente economico che sembra gratuito ed è rapidissimo. La posta elettronica è un nuovo canale di accesso alla nostra persona, attivo costantemente, che ci serve sul lavoro e nella vita privata. Purtroppo chi ha sviluppato il sistema dell'e-mail non ha pensato a porre preventivamente le condizioni per evitare o punire gli abusi. Lo spirito di collaborazione e di apertura che ha caratterizzato Internet, soprattutto all'inizio, non ha permesso ai pionieri della Rete di immaginare le possibilità per sfruttarla in modo inappropriato. Altri motivi non hanno consentito di prevedere gli abusi: alcune implicazioni della posta elettronica sono diventate evidenti con il passare degli anni; l'accesso a persone di culture diverse (anche di culture di marketing) che fanno un uso diverso di Internet e dell'e-mail e la rapidità con cui queste tecnologie si sono diffuse, hanno impedito di rendersi conto chiaramente di cosa fosse un abuso e cosa no. La cultura non si è diffusa insieme al mezzo. E quando ci si è accorti del problema, ormai era tardi.

Con il trascorrere degli anni lo spamming si è diffuso, ma ancor oggi non è stato chiaramente definito, identificato e condannato: abbiamo visto come la definizione di spamming sia nebulosa. La necessità di dare una giustificazione o almeno una dimensione etica alla lotta contro lo spamming è una prova del fatto che lo spamming non è universalmente recepito come problema. Per rinforzare questo concetto propongo un paragone. Consideriamo le seguenti situazioni: un predicatore di qualche religione suona alla nostra porta ogni mezz'ora; un operatore marketing ci chiama a casa in piena notte, ripetutamente; un candidato alle elezioni ci invia quotidianamente il suo programma via posta cartacea. Tutte queste situazioni sono universalmente considerate abusi. Abusi della nostra libertà di disporre del nostro tempo e del nostro spazio. In questo senso, la nozione di spamming come abuso non è così chiara.

Lo spamming è un fenomeno che nasce da un uso inappropriato della tecnologia. La tecnologia ci mette a disposizione possibilità comunicative fantastiche, ma al tempo stesso ci rende bersagli di un'aberrazione di sé stessa, di un uso sconsiderato e illegittimo che rischia di mettere a repentaglio l'intero sistema. La posta elettronica è una tecnologia che potrebbe soccombere a se stessa. Tuttavia sono ottimista: «L'evoluzione della rete è biologica. Può essere veloce, ma ha tempi e ritmi che seguono un'evoluzione naturale.» scrive Giancarlo Livraghi<sup>1</sup>. Tutti gli organismi biologici hanno trovato un equilibrio. Servono anni e dure lotte, ma alla fine la natura impone la sua legge.

E qualcosa si sta già muovendo. Gli addetti ai lavori si sono resi conto del problema e ci stanno lavorando, ma hanno bisogno di appoggio perché le implicazioni dello spamming non sono solo tecniche. Soprattutto, ciò che serve è una chiara definizione di spamming e di un mezzo per punire gli abusi. Per questo è necessario che l'opinione pubblica si confronti con il problema e con tutte le sue implicazioni, in modo che la politica sia spinta a dare quegli strumenti che solo essa può dare: definizioni e leggi. E poi soldi: il freno agli investimenti nel campo delle tecnologie dell'informazione e della comunicazione toglie le risorse necessarie alla gestione delle infrastrutture e porta a problemi non solo collegati allo spamming, ma anche alla sicurezza, ai virus e a molte altre cose.

Brad Templeton ripete che, comunque, è solo spamming. Come ho riferito in questo lavoro, lo spamming è uno dei problemi di Internet e non è il peggiore, probabilmente. Questa opinione non è condivisa da tutti: il presidente di un piccolo ISP americano ritiene che la situazione sia molto sottovalutata. «Spam is a thousand times more horrible than you can ever imagine, the

---

<sup>1</sup> **Giancarlo Livraghi**, *Il Mercante in Rete*, numero 52, 10 novembre 2000, <http://www.gandalf.it/mercante/merca52.htm> (consultato il 5 aprile 2002)

entire Internet mail system is under a denial-of-service attack.»<sup>2</sup> Ma affrontare lo spamming come problema costringe anche a riflettere su cosa è lecito e cosa non lo è, costringe a chiedersi fino a dove arriva la nostra libertà di starcene in pace e fino a dove, invece, va la nostra libertà di comunicare. Se un giorno avremo leggi sullo spamming sbagliate, ogni volta che spediremo un e-mail potremmo doverci chiedere se ciò che stiamo facendo è illegale. Perdere la possibilità di comunicare con gli estranei è una rinuncia che non dobbiamo permetterci: «Non tutti i messaggi inaspettati sono indesiderabili, anzi... spesso è molto interessante ricevere posta inattesa e così incontrare persone nuove.»<sup>3</sup> scrive ancora Livraghi. Per questo ho ritenuto importante considerare anche l'aspetto legale del fenomeno: è nell'ambito della legge e della politica che questa battaglia tra libertà va combattuta. Non è una questione che riguarda (solo) i tecnici.

Non mi azzardo a fare previsioni precise per il futuro, ma non è difficile indicare alcuni scenari probabili: lo spamming crescerà e si arricchirà di immagini e suoni, come talvolta già succede. E troverà altri spazi nei nuovi canali di comunicazione che si apriranno o si perfezioneranno. Oggi riceviamo sui nostri telefonini degli SMS che potremmo considerare spamming, o comunque un parente dello spamming. L'arrivo della nuova versione degli SMS, gli MMS, verrà sicuramente sfruttato anche dagli spammer. Se nei prossimi anni assisteremo alla convergenza di tecnologie oggi distinte come Internet e la comunicazione mobile, allora potremo anche ammirare quali altre opere fantasiose metteranno in atto i protagonisti dello spam.

Nonostante, e lo ripeto, la definizione di spamming non tenga conto del contenuto del messaggio, è innegabile che il marketing è un motore forte. Potrebbe sembrare che basti regolamentare l'aspetto pubblicitario, come certi politici vorrebbero, per limitare il fenomeno entro limiti tollerabili. Questo però potrebbe condurre a una sorta di legittimazione. E comunque non basta: oggi è la pubblicità, domani cos'altro? Infatti bisogna ricordare che il mondo pubblicitario è in forte evoluzione. All'inizio la funzione primaria della pubblicità era quella di fornire informazioni ai consumatori orfani di quegli empori di quartiere che erano crollati sotto il peso della grande distribuzione. Con gli anni il ruolo della pubblicità e delle altre forme di marketing è diventato "solo" quello di creare il brand, un ruolo meno pratico e più emozionale. Oggi il consumatore si sta rendendo conto che se vuole informazioni le può trovare. A dispetto delle corporation che vorrebbero controllarlo, sa anche dove procurarsele. Non è più necessario

---

<sup>2</sup> « Lo spam è mille volte più terribile di quanto si possa immaginare, l'intero sistema di posta su Internet è sotto un attacco di tipo denial-of-service.» **Mitch Wagner**, *ISP Chief: Spam Is 'A Thousand Times More Horrible Than You Can Imagine'*, op. cit.

<sup>3</sup> **Giancarlo Livraghi**, 27. *Pressatelle poco gustose e pasticcini un po' indigesti*, maggio 1998, in *Portolano Italiano*, [http://www.gandalf.it/net/portolan/port\\_27.htm](http://www.gandalf.it/net/portolan/port_27.htm) (consultato il 5 aprile 2002).

ripetergli continuamente le stesse cose. Al contrario, lo spamming è un'espressione del direct marketing, dove è l'azienda a fornire le informazioni su ciò che essa ritiene interessi al consumatore. Il direct marketing tradizionale ha fallito anche sotto altri punti di vista: la segmentazione dei consumatori si è rivelata un compito arduo, ha portato a creare dei consensi fittizi e a definire categorie così poco selettive da essere inutilizzabili.

Io sono convinto che si possa fare marketing in Rete, ma per ottenere o mantenere la credibilità è necessario stare il più lontani possibile dallo spamming, cosa che sarà possibile solo con definizioni chiare: non conta vendere una volta, ma acquisire clienti, costruire relazioni, conquistare fiducia. Le marche importanti e le imprese qualificate l'hanno capito e lo spamming è lo strumento usato solo dagli ingenui o dagli imbroglioni.

## 10. Indici delle tabelle e delle figure

### 10.1. Indice delle tabelle

Tabella 1: categorie di spam secondo Brightmail	13
Tabella 2: elenco indirizzi generati automaticamente	56
Tabella 3: newsletter, situazione dopo un anno	103
Tabella 4: Usenet e web, pubblicazione degli indirizzi	105
Tabella 5: Usenet e web, risultati globali al 19 novembre 2002	107
Tabella 6: generazione automatica, confronto tra indirizzi	113
Tabella 7: lingua dei messaggi, confronto tra indirizzi	113
Tabella 8: risultati filtri anti-spam	114

### 10.2. Indice delle figure

Figura 1: categorie di spam secondo Brightmail	14
Figura 2: schema dei protocolli della posta elettronica	24
Figura 3: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su <i>ch.comp.os.linux</i>	109
Figura 4: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su <i>comp.mail.pine</i>	109
Figura 5: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su <i>it.hobby.cucina</i>	110
Figura 6: grafico dei messaggi di spam ricevuti per gli indirizzi pubblicati su <i>alt.alcohol</i>	110
Figura 7: confronto tra i gruppi di discussione	112

## 11. Bibliografia

### 11.1. Siti web

- **Adberg Consulting LCC**, <http://www.adbergllc.com/>
- **Brightmail**, <http://www.brightmail.com/>
- **CAUCE**, <http://www.cauce.org/>
- **Cloudmark**, <http://www.cloudmark.com/>
- **Despammed**, <http://www.despammed.com/>
- **drbcheck**, <http://moensted.dk/spam/>
- **EuroCAUCE**, <http://www.euro.cauce.org/>
- **Fighters4web**, <http://www.fighters4web.com/>
- **Incaricato federale per la protezione dei dati**, <http://www.edsb.ch/i/>
- **Information zum Thema Spam**, <http://spam.trash.net/>
- **MAPS**, <http://www.mail-abuse.org/>
- **Merriam-Webster**, <http://www.m-w.com/dictionary.htm>
- **NoSpamWare**, <http://www.nospamware.it/>
- **ORDB**, <http://www.ordb.org/>
- **Pagina Antispam in italiano**, <http://www.collinelli.net/antispam/>
- **Petemoss.com**, <http://www.petemoss.com/>
- **SamSpade**, <http://samspade.org/>
- **Slashdot**, <http://slashdot.org/>
- **spam.abuse.net**, <http://spam.abuse.net/>
- **Spam Archive**, <http://www.spamarchive.org/>
- **Spam Arrest**, <http://www.spamarrest.com/>
- **SpamAssassin**, <http://eu.spamassassin.org/>
- **SpamBouncer**, <http://www.spambouncer.org/>
- **spam-ch**, <http://www.verboten.net/mailman/listinfo/spam-ch>
- **SpamCop**, <http://www.spamcop.net/>
- **SpamCon Foundation**, <http://www.spamcon.org/>
- **Spam Conference**, <http://www.spamconference.org/>
- **SpamEater**, <http://www.hms.com/spameater.asp>

- **Spamex**, <http://www.spamex.com/>
- **spamfaq.net**, <http://www.spamfaq.net/>
- **Spamhaus**, <http://www.spamhaus.org/>
- **SpamKiller**, <http://www.mcafee.com/myapps/msk/default.asp>
- **Spamlaw**, <http://www.spamlaw.com/>
- **SpamPal**, <http://www.spampal.org.uk/>
- **Spam Recycling Center**, <http://www.spamrecycle.com/>
- **Spam Terminator**, <http://www.sertel.net/terminator/>
- **Spews**, <http://www.spews.org/>
- **UXN Spam Combat**, <http://combat.uxn.com/>
- **Vipul's Razor**, <http://razor.sourceforge.net/>

## 11.2. Libri

- **Giancarlo Livraghi**, *L'umanità dell'internet (le vie della rete sono infinite)*, Milano, Hops, 2001
- **Armand Mattelart**, *La comunicazione globale*, Roma, Editori Riuniti, 1998

## 11.3. Leggi, decreti e direttive

- *Decisione dell'11 gennaio 2001, Raccolta e trattamento di caselle di posta elettronica attraverso procedure di spamming per comunicazioni politiche*, <http://www.interlex.it/testi/d010111.htm> (consultato il 19 novembre 2002)
- *Decreto legislativo 13 maggio 1998, n. 171*, <http://www.interlex.it/testi/dlg98171.htm> (consultato il 18 novembre 2002)
- *Decreto legislativo 22 maggio 1999, n. 185*, <http://www.interlex.it/testi/dlg99185.htm> (consultato il 18 novembre 2002)
- *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, [http://www.interlex.it/testi/02\\_58ce.htm](http://www.interlex.it/testi/02_58ce.htm) (consultato il 19 novembre 2002)
- *Legge Federale del 19 giugno 1992 sulla protezione dei dati (LPD)*, [http://www.admin.ch/ch/i/rs/c235\\_1.html](http://www.admin.ch/ch/i/rs/c235_1.html) (consultato il 19 novembre 2002)

## 11.4. Articoli

- **ACSI**, *Pubblicità indesiderata*, <http://www.acsi.ch/enc/enc.cfm?scheda=101> (consultato il 13 novembre 2002)
- **Vittorio Bertola**, *Usenet Death Penalty FAQ*, 4 novembre 1998, [http://digilander.libero.it/mamoFAQ/FAQ-udp\\_i.txt](http://digilander.libero.it/mamoFAQ/FAQ-udp_i.txt) (consultato il 29 ottobre 2002)
- **Lisa M. Bowman**, *Washington court: Don't spam our residents*, 7 giugno 2001, in CNET Tech News, <http://news.com.com/2100-1023-268045.html?legacy=cnet> (consultato il 23 agosto 2002)
- **Giuseppe Briganti**, *Spamming e diritto - L'invio di messaggi di posta elettronica non richiesti*, 29 dicembre 2001, in Ius Reporter, <http://www.iusreporter.it/Testi/doc-spamming.htm> (consultato il 19 novembre 2002)
- **Manlio Cammarata**, *Qualcosa si muove contro "spammers" e spioni*, 12 settembre 2002, in InterLex, <http://www.interlex.it/675/qualcosa.htm> (consultato il 18 novembre 2002)
- **CAUCE**, *The Problem*, <http://www.cauce.org/about/problem.shtml> (consultato il 3 agosto 2002)
- **CAUCE**, *Cauce does the math - Why can't the marketing industry?*, <http://www.cauce.org/pressreleases/math.shtml>, 15 maggio 2001 (consultato il 3 agosto 2002)
- **Massimo Cavazzini**, *Combattere lo spam, come colpire gli spammer al portafogli*, <http://www.maxkava.com/spam/> (consultato il 14 novembre 2002)
- **Richard Clayton**, *Good practice for combating Unsolicited Bulk Email*, 18 maggio 1999, <http://www.ripe.net/ripe/docs/ripe-206.html> (consultato il 2 gennaio 2003)
- **David H. Crocker**, *RFC-822: Standard for the format of arpa internet text messages*, 13 agosto 1982, <http://www.ietf.org/rfc/rfc822.txt> (consultato il 15 settembre 2002)
- **Paolo De Andreis** (a cura di), *Interviste/ L'umanità dell'internet*, 6 luglio 2001, in Punto Informatico, <http://punto-informatico.it/p.asp?i=36721> (consultato il 1 giugno 2002)
- **Antonio De Florio**, *Italia, il paradiso delle catene*, 28 luglio 2002, in Il Messaggero OnLine, [http://ilmessaggero.caltanet.it/hermes/20020728/01\\_NAZIONALE/INTERNI/Aaa.htm](http://ilmessaggero.caltanet.it/hermes/20020728/01_NAZIONALE/INTERNI/Aaa.htm) (consultato il 3 ottobre 2002)
- **Michelle Delio**, *Not all Asian E-Mail is spam*, 19 febbraio 2002, in Wired News, <http://www.wired.com/news/politics/0,1283,50455,00.html> (consultato il 2 gennaio 2003)
- **Polly Esther Fabrique**, *The Amazing SPAM Homepage*, <http://www.cusd.claremont.edu/~mrosenbl/spam.html> (consultato il 2 agosto 2002)

- **Federal Trade Commission**, *FTC Names Its Dirty Dozen: 12 Scams Most Likely to Arrive Via Bulk Email*, <http://www.ftc.gov/bcp/online/pubs/alerts/doznalrt.htm> (consultato il 15 luglio 2002)
- **Sharael Feist**, *The father of modern spam speaks*, 26 marzo 2002, in CNET Tech News, <http://news.com.com/2008-1082-868483.html> (consultato il 23 ottobre 2002)
- **Adriana Galgano e Eugenio La Mesa**, *Definizione di Email Marketing*, <http://www.bcentral.it/emailmarketing/definizione.asp?ii=1> (consultato il 10 novembre 2002)
- **Dan Garcia**, *SPAM*, <http://www.cs.berkeley.edu/~ddgarcia/spam.html> (consultato il 2 agosto 2002)
- **Simson Garfinkel**, *Spam King*, febbraio 1996, in Wired, <http://www.wired.com/wired/4.02/spam.king.html> (consultato il 24 ottobre 2002)
- **Sharon Gaudin e Suzanne Gaspar**, *The Spam police*, 10 settembre 2001, in Network World, <http://www.nwfusion.com/research/2001/0910feat.html> (consultato il 30 dicembre 2002)
- **Serge Gauthronet, Etienne Drouard**, *Unsolicited Commercial Communications and Data Protection (Internal Market DG – Contract n° ETD/99/B5 -3000/E/96)*, gennaio 2001, [http://europa.eu.int/comm/internal\\_market/en/dataprot/studies/spamstudyen.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamstudyen.pdf) (consultato il 5 agosto 2002)
- **Serge Gauthronett & Étienne Drouard**, *Messaggi pubblicitari indesiderati e protezione dei dati personali, Sintesi delle conclusioni dello studio*, gennaio 2001, [http://europa.eu.int/comm/internal\\_market/en/dataprot/studies/spamsumit.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/studies/spamsumit.pdf) (consultato il 5 agosto 2002)
- **T. Gavin**, *RFC-3098: How to Advertise Responsibly Using E-Mail and Newsgroups or - how NOT to \$\$\$\$ MAKE ENEMIES FAST! \$\$\$\$*, aprile 2001, <http://www.ietf.org/rfc/rfc3098.txt> (consultato il 15 settembre 2002)
- **Paul Graham**, *A plan for spam*, agosto 2002, <http://www.paulgraham.com/spam.html> (consultato il 2 dicembre 2002)
- **Paul Graham**, *Filters vs. Blacklists*, settembre 2002, <http://www.paulgraham.com/falsepositives.html> (consultato il 30 dicembre 2002)
- **Gruppo per la tutela dei dati personali (Unione Europea)**, *Raccomandazione relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea*, 17 maggio 2002, [http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp43it.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp43it.pdf) (consultato il 5 settembre 2002)

- **Gruppo per la tutela dei dati personali (Unione Europea)**, *Parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali*, 3 febbraio 2000, [http://europa.eu.int/comm/internal\\_market/en/dataprot/wpdocs/wp28it.pdf](http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp28it.pdf) (consultato il 5 settembre 2002)
- **Julian Haight**, *On what type of email should I (not) use SpamCop?*, <http://spamcop.net/fom-serve/cache/14.html> (consultato il 6 agosto 2002)
- **S. Hambridge**, *RFC-1855: Netiquette Guidelines*, ottobre 1995, <http://www.ietf.org/rfc/rfc1855.txt> (consultato il 15 settembre 2002)
- **Paul Hoffman**, *Unsolicited Bulk Email: Definitions and Problems (Internet Mail Consortium Report: UBE-DEF IMCR-004)*, 5 ottobre 1997, <http://www.imc.org/ube-def.html> (consultato il 16 giugno 2002)
- **Paul Hoffman, Dave Crocker**, *Unsolicited Bulk Email: Mechanism for Control (Internet Mail Consortium Report: UBE-SOL IMCR-008)*, 4 maggio 1998, <http://www.imc.org/ube-sol.html> (consultato il 16 giugno 2002)
- **Hormel**, *SPAM and the Internet*, [http://www.spam.com/ci/ci\\_in.htm](http://www.spam.com/ci/ci_in.htm) (consultato il 2 agosto 2002)
- **M. Horton**, *RFC-1036: Standard for Interchange of USENET Messages*, dicembre 1987, <http://www.ietf.org/rfc/rfc1036.txt> (consultato il 15 settembre 2002)
- **Infinite Monkeys & Company**, *Spam defined*, <http://www.monkeys.com/spam-defined/definition.shtml> (consultato il 16 luglio 2002)
- **Philip Jacob**, *The Spam Problem, Moving beyond RBLs*, 30 dicembre 2002, <http://theory.whirlycott.com/~phil/antispam/rbl-bad/rbl-bad.html> (consultato il 2 gennaio 2003)
- **Reshma Kapadia**, *'Spam' Likely to Clutter E-Mail for Some Time*, 2 dicembre 2002, in Yahoo! News, [http://story.news.yahoo.com/news?tmpl=story&u=/nm/20021202/wr\\_nm/tech\\_spam\\_dc\\_4](http://story.news.yahoo.com/news?tmpl=story&u=/nm/20021202/wr_nm/tech_spam_dc_4) (consultato il 19 dicembre 2002)
- **Mo Krochmal**, *Spammer Says "Uncle" To AOL*, in TechWeb News, 19 dicembre 1997, <http://content.techweb.com/wire/story/TWB19971218S0007> (consultato il 2 agosto 2002)
- **Lawrence Lessig**, *A bounty on spammers*, 16 settembre 2002, in CIO Insight, <http://www.cioinsight.com/article2/0,3959,533225,00.asp> (consultato il 7 gennaio 2003)
- **Lawrence Lessig**, *Putting my job where my mouth is*, 1 gennaio 2003, in Lessig Blog, [http://cyberlaw.stanford.edu/lessig/blog/archives/2003\\_01.shtml#000787](http://cyberlaw.stanford.edu/lessig/blog/archives/2003_01.shtml#000787) (consultato il 7 gennaio 2003)

- **John Leyden**, *Hotmail, Yahoo! erect roadblocks for spam sign-ons*, 27 dicembre 2002, in The Register, <http://www.theregister.co.uk/content/6/28694.html> (consultato il 7 gennaio 2003)
- **G. Lindberg**, *RFC-2505: Anti-Spam Recommendations for SMTP MTAs*, febbraio 1999, <http://www.ietf.org/rfc/rfc2505.txt> (consultato il 15 settembre 2002)
- **G. Lindberg**, *RFC-2635: DON'T SPEW, A Set of guidelines for mass unsolicited mailings and postings (spam\*)*, giugno 1999, <http://www.ietf.org/rfc/rfc2635.txt> (consultato il 15 settembre 2002)
- **Giancarlo Livraghi**, *Gandalf, pensieri sulla rete e sulla comunicazione*, <http://www.gandalf.it/>
- **Giancarlo Livraghi**, *Il Mercante in Rete*, numero 52, 10 novembre 2000, <http://www.gandalf.it/mercante/merca52.htm> (consultato il 5 aprile 2002)
- **Giancarlo Livraghi**, *27. Pressatelle poco gustose e pasticcini un po' indigesti*, maggio 1998, in *Portolano Italiano*, [http://www.gandalf.it/net/portolan/port\\_27.htm](http://www.gandalf.it/net/portolan/port_27.htm) (consultato il 5 aprile 2002)
- **Rick Lockridge**, *Congress has hard time stomaching e-mail spam*, 14 maggio 2001, in CNN.com, <http://www.cnn.com/2001/TECH/internet/05/14/spam.wars/index.html> (consultato il 3 agosto 2002)
- **Mylene Mandalindan**, *For Bulk E-Mailer, Pestering Millions Offers Path to Profit*, 13 novembre 2002, in The Wall Street Journal Online, [http://online.wsj.com/article\\_email/0,,SB1037138679220447148,00.html](http://online.wsj.com/article_email/0,,SB1037138679220447148,00.html) (consultato il 14 novembre 2002)
- **Nancy McGough**, *Reverse spam filtering - Winning Without Fighting*, 4 settembre 2002, <http://www.ii.com/internet/messaging/spam/> (consultato il 2 dicembre 2002)
- **Infinite Monkeys & Company**, *Spam defined*, <http://www.monkeys.com/spam-defined/definition.shtml> (consultato il 16 luglio 2002)
- **Andrea Monti**, *Spam e indirizzi e-mail. Quando la 675 è impotente*, 15 febbraio 2001, in InterLex, <http://www.interlex.it/675/amonti44.htm> (consultato il 18 novembre 2002)
- **Scott Hazen Mueller** (trad. Giulio Pipitone), *What is spam?*, <http://www.fighters4web.com/pagine/mirror/What%20is%20spam.htm> (consultato il 17 ottobre 2002)
- **Network Associates Inc.**, *Press Release Source: Network Associates Acquires Deersoft, Inc. Anti-Spam Technology*, in YahooFinance, 6 gennaio 2002, [http://biz.yahoo.com/prnews/030106/sfm029\\_1.html](http://biz.yahoo.com/prnews/030106/sfm029_1.html) (consultato il 7 gennaio 2002)

- **Open Directory Project**, *Open Directory Editorial Guidelines: spamming*, <http://dmoz.org/guidelines/spamming.html> (consultato il 17 luglio 2002)
- **Giulio Pipitone**, *Rapporto su situazione "prevenzione spam" sui newsgroup*, marzo 2002, <http://www.fighters4web.com/pagine/esperimenti/studiomarzo.html> (consultato il 22 ottobre 2002)
- **Jonathan B. Postel**, *RFC-821: Simple Mail Transfer Protocol*, agosto 1982, <http://www.ietf.org/rfc/rfc821.txt> (consultato il 15 settembre 2002)
- **Andrea Putignani**, *Consenso, informativa e direct marketing*, 17 maggio 2001, in InterLex, <http://www.interlex.it/675/putigna1.htm> (consultato il 18 novembre 2002)
- **Scarlett Pruitt**, *Will new filters save us from spam?*, 17 gennaio 2003, in InfoWorld, <http://www.infoworld.com/articles/hn/xml/03/01/17/030117hnsppammit.xml?s=IDGNS> (consultato il 20 gennaio 2003)
- **Eric Raymond**, *Jargon File*, <http://www.tuxedo.org/~esr/jargon/> (consultato il 2 agosto 2002)
- **Redazione Interlex**, *Tutela dei dati personali - Legge 675/96*, in Interlex, <http://www.interlex.it/675/indice.htm> (consultato il 18 novembre 2002)
- **Redazione Punto Informatico**, *200 mln di email al giorno in Italia*, 20 dicembre 2002, in Punto Informatico, <http://punto-informatico.it/p.asp?i=42580> (consultato il 20 dicembre 2002)
- **Redazione Punto Informatico**, *Sorpresa..? Un'email su sei è spam*, 18 ottobre 2002, in Punto Informatico, <http://punto-informatico.it/p.asp?i=41819> (consultato il 20 dicembre 2002)
- **Melissa Solomon**, *The Other Side*, 11 novembre 2002, in Computerworld, <http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,75736,0.html> (consultato il 28 novembre 2002)
- **SIUG - Swiss Internet User Group**, *Positionspapier zum Thema Spam*, 11 settembre 1999, <http://www.siug.ch/positionen/SIUG-Spam.shtml> (consultato il 12 novembre 2002)
- **The Skeptical Mind**, *A rash of illegal spam attempts have wrongly implicated this website!*, <http://www.skepticalmind.com/> (consultato il 18 luglio 2002)
- **Stewart Taggart**, *Spam Blockers Pass It On*, 2 luglio 2001, in Wired, <http://www.wired.com/news/culture/0,1284,44876-2,00.html> (consultato il 30 dicembre 2002)
- **Brad Templeton**, *Essays on Junk E-mail (Spam)*, <http://www.templetons.com/brad/spume/> (consultato il 24 ottobre 2002)

- **US Equity & Macro LAB staff**, *The Ponzi Scheme*,  
[http://www.usemlab.com/html/commenti/archivio\\_commenti/quadrogenerale/QG\\_02\\_05\\_15.htm](http://www.usemlab.com/html/commenti/archivio_commenti/quadrogenerale/QG_02_05_15.htm) (consultato il 10 agosto 2002)
- **Mike Wendland**, *Internet spammer can't take what he dishes out*, 6 dicembre 2002, in Detroit Free Press, [http://www.freep.com/money/tech/mwend6\\_20021206.htm](http://www.freep.com/money/tech/mwend6_20021206.htm) (consultato il 18 dicembre 2002)
- **Mike Wendland**, *Spam king lives large off others' e-mail troubles*, 22 novembre 2002, in Detroit Free Press, [http://www.freep.com/money/tech/mwend22\\_20021122.htm](http://www.freep.com/money/tech/mwend22_20021122.htm) (consultato il 24 novembre 2002)
- **Yahoo Help**, *Che cos'è lo spam?*, <http://help.yahoo.com/help/it/mail/spam/spam-02.html> (consultato l'8 agosto 2002)
- **Mitch Wagner**, *ISP Chief: Spam Is 'A Thousand Times More Horrible Than You Can Imagine'*, 19 dicembre 2002, in InternetWeek.com, <http://www.internetwk.com/story/INW20021219S0003> (consultato il 20 dicembre 2002)

## 12. Allegati

### 12.1. Citazioni originali

In questo capitolo riporto tutte le citazioni che nel testo sono state tradotte in italiano.

#### Pagina 6:

«spam (noun): unsolicited usually commercial E-mail sent to a large number of addresses»

Fonte: **Merriam-Webster**, op. cit.

\*\*\*

#### Pagina 6:

«spam vt.,vi.,n. [from “Monty Python’s Flying Circus”]

To crash a program by overrunning a fixed-size buffer with excessively large input data. See also buffer overflow, overrun screw, smash the stack.

To cause a newsgroup to be flooded with irrelevant or inappropriate messages. You can spam a newsgroup with as little as one well- (or ill-) planned message (e.g. asking “What do you think of abortion?” on soc.women). This is often done with cross-posting (e.g. any message which is cross-posted to alt.rush-limbaugh and alt.politics.homosexuality will almost inevitably spam both groups). This overlaps with troll behavior; the latter more specific term has become more common.

To send many identical or nearly-identical messages separately to a large number of Usenet newsgroups. This is more specifically called ‘ECP’, Excessive Cross-Posting. This is one sure way to infuriate nearly everyone on the Net. See also velveeta and jello.

To bombard a newsgroup with multiple copies of a message. This is more specifically called ‘EMP’, Excessive Multi-Posting.

To mass-mail unrequested identical or nearly-identical email messages, particularly those containing advertising. Especially used when the mail addresses have been culled from network traffic or databases without the consent of the recipients. Synonyms include UCE, UBE.

Any large, annoying, quantity of output. For instance, someone on IRC who walks away from their screen and comes back to find 200 lines of text might say “Oh no, spam”.

The later definitions have become much more prevalent as the Internet has opened up to non-techies, and to most people senses 3 4 and 5 are now primary. All three behaviors are considered abuse of the net, and are almost universally grounds for termination of the originator's email account or network connection. In these senses the term 'spam' has gone mainstream, though without its original sense or folkloric freight - there is apparently a widespread myth among lusers that "spamming" is what happens when you dump cans of Spam into a revolving fan. Hormel, the makers of Spam, have published a surprisingly enlightened position statement on the Internet usage.»

Fonte: **Eric Raymond**, *Jargon File*, op. cit.

\*\*\*

#### **Pagina 8:**

«Spam occurs if identical pages are submitted to the same category multiple times, if one site is submitted to multiple inappropriate categories, or if a submission otherwise violates our Submission Policies or disrupts the ODP.»

Fonte: **Open Directory Project**, *Open Directory Editorial Guidelines: spamming*, op. cit.

\*\*\*

#### **Pagina 8:**

«For me spam must be:

1. unsolicited (I didn't request it), and
2. automated (this same email was sent to thousands of people at once).»

Fonte: **Julian Haight**, *On what type of email should I (not) use SpamCop?*, op. cit.

\*\*\*

#### **Pagina 9:**

«I define E-mail abuse to be mail that meets all three of these criteria:

1. It is unsolicited
2. It is part of a "mass mailing." (bulk mail)
3. The sender is a stranger to the recipient. (The recipient has never had wilful personal contact with the sender.)»

Fonte: **Brad Templeton**, *Essays on Junk E-mail (Spam)*, op. cit.

\*\*\*

**Pagina 10:**

«Internet spam is one or more unsolicited (1) messages, sent or posted as part of a larger collection (2) of messages, all having substantially identical content (3).»

Fonte: **MONKEYmedia**, *Spam defined*, op. cit.

\*\*\*

**Pagina 12:**

«The term “spam” refers broadly to unsolicited bulk e-mail (or “junk e-mail”), which “can be either commercial (such as an advertisement) or noncommercial (such as a joke or chain letter).”»

Fonte: **MONKEYmedia**, *Spam defined*, op. cit.

\*\*\*

**Pagina 43:**

«Finally, let us make some projections of volumes and costs. There are currently 234 million Internet users worldwide and this figure is likely to reach 300 million by the end of 2000. If it is assumed that sooner or later every e-mail marketer will acquire the technical capacity to transmit 100 million e-mails daily, Internet users could potentially be overwhelmed by the resulting flood of messages – 200 senders with that sort of capacity could mean 20 billion commercial e-mails being sent every day. Every web surfer would receive an average of over 60 emails a day, representing a total download time of approximately 1 hour with current technology. And this is without taking account of the increasing use of photographic and video content in commercial e-mails. Is there not a real risk of Internet entropy if steps are not taken expeditiously to introduce the necessary degree of regulation? An extremely rigorous interpretation of the opt-in concept would appear vital to the system’s survival.»

Fonte: **Serge Gauthronet, Etienne Drouard**, *Unsolicited Commercial Communications and Data Protection (Internal Market DG – Contract n° ETD/99/B5 -3000/E/96)*, op. cit.

## **12.2. Netiquette: etica e norme di buon uso dei servizi di rete**

Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, ed in particolare fra i lettori dei servizi di “news” Usenet, si sono sviluppati nel corso del tempo una serie di “tradizioni” e di “principi di buon comportamento” (galateo) che vanno collettivamente sotto il nome di “netiquette”. Tenendo ben a mente che la entità che fornisce l'accesso ai servizi di rete (provider, istituzione pubblica, datore di lavoro, etc.) può regolamentare in modo ancora più preciso i doveri dei propri utenti, riportiamo in questo documento un breve sunto dei principi fondamentali della “netiquette”, a cui tutti sono tenuti ad adeguarsi.

1. Quando si arriva in un nuovo newsgroup o in una nuova lista di distribuzione via posta elettronica, è bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi in giro per il mondo: in tale modo ci si rende conto dell'argomento e del metodo con cui lo si tratta in tale comunità.
2. Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema.
3. Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione.
4. Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale.
5. Non condurre “guerre di opinione” sulla rete a colpi di messaggi e contromessaggi: se ci sono diatribe personali, è meglio risolverle via posta elettronica in corrispondenza privata tra gli interessati.
6. Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica.
7. Non pubblicare messaggi stupidi o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione. Leggere sempre le FAQ (Frequently Asked Questions) relative all'argomento trattato prima di inviare nuove domande.
8. Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito.
9. Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso:

- A. La rete è utilizzata come strumento di lavoro da molti degli utenti. Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.
- B. Qualunque attività che appesantisca il traffico sulla rete, quale per esempio il trasferimento di archivi voluminosi, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in orari diversi da quelli di massima operatività (per esempio di notte), tenendo presenti le eventuali differenze di fuso orario.
- C. Vi sono sulla rete una serie di siti server (file server) che contengono in copia aggiornata documentazione, software ed altri oggetti disponibili sulla rete. Informatevi preventivamente su quale sia il nodo server più accessibile per voi. Se un file è disponibile su di esso o localmente, non vi è alcuna ragione per prenderlo dalla rete, impegnando inutilmente la linea e impiegando un tempo sicuramente maggiore per il trasferimento.
- D. Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o redistribuirlo in qualunque modo e sotto qualunque forma.
- E. Comportamenti palesemente scorretti da parte di un utente, quali:
  - violare la sicurezza di archivi e computers della rete;
  - violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
  - compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente;costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge.

Per chi desiderasse approfondire i punti qui trattati, il documento di riferimento è RFC1855 “Netiquette Guidelines”, ed anche RFC2635 “A Set of Guidelines for Mass Unsolicited Mailings and Postings” disponibili sulla rete presso:

<ftp://ftp.nic.it/rfc/rfc1855.txt>

<ftp://ftp.nic.it/rfc/rfc2635.txt>

### 12.3. Gennaio 2003: Spam Conference

Il 17 gennaio 2003, presso il Massachusetts Institute of Technology, si è tenuta la prima Spam Conference<sup>1</sup>. Circa cinquecento programmatori, ricercatori e hacker hanno partecipato come spettatori, mentre i venti relatori erano accademici, consulenti indipendenti e rappresentanti di aziende. Tra essi Paul Graham (autore del primo algoritmo anti-spam basato sulla probabilità bayesiana, trattato anche in questa memoria), Eric Raymond (che ha scritto la prima implementazione in C dell'algoritmo di Paul Graham, chiamata Bogofilter), Ken Schneider di Brightmail e Matt Sergeant di MessageLabs. Mi sono fatto un'idea di cosa è stato discusso dall'abstract degli interventi, alcuni dei quali li ho seguiti grazie al web-cast live.

Lo scopo dichiarato di questa conferenza è quello di trovare una soluzione, un filtro tanto efficace da azzerare le risposte agli spammer in modo da annullare i loro guadagni.

Il problema è considerato importante da tutti gli operatori e viene anche definito un problema di sicurezza delle informazioni. Si sente la mancanza di una definizione comune, in particolare tra utenti privati e tra privati e ISP.

Molti relatori hanno descritto alcune tecniche basate sulla probabilità bayesiana, che sembra essere la strada futura. Sia Paul Graham che altri hanno proposto miglioramenti all'algoritmo bayesiano implementato dallo stesso Graham, ma viene anche sottolineata l'importanza di filtri che si adattano in tempo reale e di sistemi che imparano, per cui mancano le relative infrastrutture di "allenamento". Questo perché lo spam è costantemente in evoluzione e molti messaggi di spam assomigliano sempre più a messaggi di non spam.

La validità di un approccio legale al problema non viene messa in discussione, anzi. Si sottolinea l'importanza di metodi di tracciamento e di archiviazione dei messaggi di spam come supporto per le cause, così come quella di contratti e di policy che permettano un filtraggio aggressivo senza intralciare i messaggi legittimi.

Tra i problemi particolari, segnalo la trattazione di quelli relativi agli ISP (più sei grosso, più clienti devi soddisfare, più in fretta gli spammer si adattano alle tue contromisure) e alle tecniche adottate per difendersi dallo spamming sulle mailing list.

Non è prevista alcuna Spam Conference per l'anno prossimo, perché gli organizzatori sperano ottimisticamente che il problema venga risolto prima. «Non voglio essere al lavoro sul problema dello spamming tra dieci anni!»<sup>2</sup> ha affermato Paul Graham.

---

<sup>1</sup> **Spam Conference**, <http://www.spamconference.org/>.

<sup>2</sup> «I don't want to be working on the spam problem ten years from now!» **Scarlett Pruitt**, *Will new filters save us from spam?*, 17 gennaio 2003, in InfoWorld, <http://www.infoworld.com/articles/hn/xml/03/01/17/030117hnsppammit.xml?s=IDGNS> (consultato il 20 gennaio 2003).