O pesadelo do SPAM

Renata Cicilini Teixeira (renata@rnp.br)

Resumo

A Internet surgiu sem grandes pretensões, voltada para interesses bem específicos: ensino e pesquisa. Hoje, na entrada no novo milênio, nos deparamos com uma rede que conecta computadores no mundo todo, usada para os mais diversos fins e por uma comunidade de usuários cada vez mais heterogênea. O comércio eletrônico é uma realidade e estamos presenciando a chamada democratização da Internet. Com certeza, este panorama tem inúmeras vantagens, mas algumas regras básicas têm se perdido. Pode-se dizer que algumas "normas de bom comportamento" ou "normas básicas de convivência em sociedade" têm sido relegadas a segundo plano por parte da comunidade virtual. Entretanto, o mau uso da rede pode tornar a vida dos milhões de usuários e profissionais da Internet um verdadeiro pesadelo. Este artigo trata de um dos maiores pesadelos da Internet atualmente: o spam, ou seja, o recebimento de mensagens não solicitadas. Verifique sua caixa postal neste momento: é praticamente impossível que você não tenha recebido hoje nenhum e-mail de propaganda, uma proposta de ganho de dinheiro fácil, ou talvez quem sabe uma corrente da sorte?

1. Introdução

Quando surgiu a idéia de escrever este artigo, fiquei em dúvida. No entanto, mudei de idéia ao abrir minha caixa postal e encontrar dezenas de mensagens não solicitadas direcionadas a mim, outras tantas vindas de usuários se queixando do aumento exponencial no volume de spam, e ainda outras vindas de administradores desesperados e revoltados solicitando informações sobre como resolver este problema.

De fato, diariamente, somos bombardeados com dezenas de mensagens eletrônicas que não solicitamos: informações sobre produtos, propagandas de sites novos espalhados pela rede, correntes da sorte, boatos diversos, etc. Todo este tráfego desnecessário, todo este "lixo" é acumulado nas caixas postais, compromete o desempenho dos servidores de correio eletrônico e da rede, além de fazer com que boa parte do nosso horário de trabalho seja destinado a limpar nossa caixa postal. Existem números espantosos com relação ao tempo gasto por profissionais todos os dias com o processamento de e-mails, a seleção de mensagens úteis dentre os tantos spams recebidos.

Muitas pessoas questionam se o spam não segue a ordem natural das coisas, afinal seria o mesmo caso dos vários folhetos de propaganda distribuidos na rua, enviados pelo correio tradicional, ou ainda dos serviços de telemarketing. Não, spam não pode ser classificado na mesma categoria que tais serviços, e a diferença básica é quem paga a conta. Raciocinando, concluímos que as empresas que fazem propaganda na rua ou pelo correio tem gastos com papel, impressão, selos, pessoal para ficar nas esquinas batendo nos vidros dos carros e etc. Da mesma forma, as empresas que utilizam a técnica do telemarketing também pagam pela propaganda feita. No caso das empresas que se utilizam do spam, quem paga a conta é quem o recebe: a vítima, pois é o destinatário acaba gastando mais tempo conectado ao seu provedor para selecionar mensagens válidas, em meio aos tantos spams recebidos diariamente, a banda do provedor e seu servidor de correio eletrônico ficam sobrecarregados com o grande volume de mensagens desnecessárias todos os dias. Além disto, para a empresa que utiliza a propaganda por spam na Internet, o método é bem atraente, já que o gasto de envio de um e-mail é o mesmo para o envio de milhares.

Antes de enveredarmos pelo submundo do spam, vale esclarecer o que é e o que não é este artigo, afinal este trata de um tema polêmico e o objetivo principal não é criar polêmica, mas sim esclarecer os usuários e administradores sobre o que

é spam, suas principais características e conseqüências, assim como mostrar algumas maneiras de se defender. Este artigo não é um tratado sobre spam e não contém receitas milagrosas para sanar todos os problemas relacionados ao assunto, mas pode ajudá-lo a diminuir o problema, caso você seja a vítima, e também a reconhecer se você não está se tornando um spammer, repassando correntes, distribuindo boatos, divulgando informações que podem não ser de interesse de seus amigos, etc.

2. O que é spam?

O termo spam, longe do mundo virtual, é, na verdade, a marca de um presunto enlatado americano (www.spam.com), que não tem relação com o envio de mensagens eletrônicas não solicitadas, exceto pelo fato de que, na série de filmes de comédia do Monty Python, alguns Vikings desajeitados pediam repetidas vezes o referido presunto.

No ambiente da Internet, spam é considerado um abuso e se refere ao envio de um grande volume de mensagens não solicitadas, ou seja, o envio de mensagens indiscriminadamente a vários usuários, sem que estes tenham requisitado tal informação. O conteúdo do spam pode ser: propaganda de produtos e serviços, pedido de doações para obras assistenciais, correntes da sorte, propostas de ganho de dinheiro fácil, boatos desacreditando o serviço prestado por determinada empresa, dentre outros. Discutiremos os tipos mais comuns de spam na próxima seção.

Com certa freqüência, os e-mails de spam são chamados de junk e-mails, ou seja, lixo. Seguindo com a terminologia, quem envia spam é chamado de spammer.

A maneira mais formal de se referir a spam é UBE, Unsolicited Bulk E-mail. Pode-se também usar o termo UCE, Unsolicited Comercial E-mail, quando se trata de spam contendo propaganda de modo geral.

3. Tipos de spam

Os tipos mais comuns de spam, considerando conteúdo e propósito, são:

Boatos e correntes

Os boatos e as correntes na Internet têm algo em comum: pedem para serem enviados a todas as pessoas que você conhece. Tais e-mails se apresentam com diversos tipos de conteúdo, sendo na maioria das vezes histórias falsas ou antigas. Para atingir seus objetivos de propagação, os boatos e correntes apelam para diversos métodos de engenharia social.

Os boatos (hoaxes) são textos que contam estórias alarmantes e falsas, que instigam o leitor a continuar sua divulgação. Geralmente, o texto começa com frases apelativas do tipo: "envie este e-mail a todos os seus amigos...". Algumas classes comuns de boatos são os que apelam para a necessidade que o ser humano possui de ajudar o próximo. Como exemplos temos os casos de crianças com doenças graves, o caso do roubo de rins, etc.

Outros tipos de boatos são aqueles que difamam empresas ou produtos, prometem brindes ou ganho de dinheiro fácil. Continuando com os exemplos, temos e-mails sobre a existência de certa substância cancerígena em determinado produto, o caso do e-mail que tratava da distribuição gratuita de telefones celulares, de viagens gratuitas a Disneyworld, etc.

Ainda dentre os boatos mais comuns na rede, pode-se citar aqueles que tratam de código malicioso, como vírus ou cavalos de tróia. Neste caso, a mensagem sempre fala de vírus poderosíssimos, capazes de destruir seu computador e assim por diante. Um dos mais famosos é o Good Times, que circulou pela rede durante anos e, de vez em quando, ainda aparece um remanescente enviado por internautas desavisados. Para maiores informações sobre boatos e vírus, consulte o site Computer Virus Myths:http://www.Vmyths.com

No Brasil, os boatos mais recentes foram sobre o roubo da Amazônia e a fiscalização de software em aeroportos. Veja mais detalhes em www.spam.org.

As correntes, chain letters, são textos que estimulam o leitor a enviar várias cópias a outras pessoas, gerando um processo contínuo de propagação. São muito semelhantes aos boatos, mas o mecanismo usado para incentivar a propagação é um pouco diferente, pois a maioria das correntes promete sorte e riqueza aos que não as interrompem e anos de má sorte e desgraça aos que se recusam a enviar N cópias do e-mail para Y pessoas nas próximas X horas! Como exemplo temos a corrente dos índios da sorte, dentre tantas outras.
O CIAC mantém um site sobre boatos e correntes em http://hoaxbusters.ciac.org.

Propagandas

Os spams com o intuito de divulgar produtos, serviços, novos sites, enfim, propaganda em geral, têm ganho cada vez mais espaço nas caixas postais dos internautas. Não é o objetivo deste artigo discutir a legitimidade da propaganda por e-mail, mas sim discutir spam, e muitas empresas tem usado este recurso para atingir os consumidores. Isto sem contar a propaganda política que inundou as caixas postais no último ano. Vale ressaltar que, seguindo o próprio conceito de spam, se recebemos um e-mail que não solicitamos, estamos sim sendo vítimas de spam, mesmo que seja um e-mail de uma super-promoção que muito nos interessa. O maior problema com a propaganda por spam é que a Internet se mostra como um meio fértil para divulgação de produtos, atinge um grande número de pessoas e a baixo custo, sendo que na verdade, quem paga a conta é quem recebe a propaganda, como discutido anteriormente.

Outros: ameaças, brincadeiras, etc.

Alguns spams são enviados com o intuito de fazer ameaças, brincadeiras de mau gosto ou apenas por diversão. Ainda assim são considerados spam. Casos de ex-namorados difamando ex-namoradas, e-mails forjados assumindo identidade alheia e aqueles que dizem: "olá, estou testando uma nova ferramenta spammer e por isto você está recebendo este e-mail", constituem alguns exemplos. Vale lembrar que não há legislação específica para casos de spam. No entanto, pode-se enquadrar certos casos nas leis vigentes no atual Código Penal Brasileiro, tais como: calúnia e difamação, falsidade ideológica, estelionato, etc.

4. Alguns artifícios usados pelos spammers

Muitos são os artifícios usados pelos spammers para convencê-lo de ter recebido um e-mail válido e não um spam, alguns dos mais usados são:

One-time e-mails

Certas mensagens dizem que serão enviados somente uma vez e que você não precisa se preocupar pois não será importunado novamente. Trata-se de spam e é bem provável que você receba outras cópias do mesmo tipo de e-mail.

"Caso não tenha interesse em continuar recebendo este tipo de mensagem, por favor solicite sua retirada de nossa lista de distribuição, enviando e-mail para remove-me-from-list@..."

Este é um dos artifícios mais freqüentes usados atualmente. São os spams do tipo "remove me". Não responda! Na verdade, ao responder você estará confirmando a legitimidade de seu e-mail e este possivelmente será inserido em malas direta de spammers pelo mundo afora.

"Se este assunto não lhe interessa, apenas delete este e-mail (Just hit delete)"

Outra categoria de disfarces usados em spam são os que pedem para serem removidos ou ignorados, caso não sejam de seu interesse. Neste caso, antes de removê-lo, siga as orientações da seção 6 deste artigo, ou seja, reclame. Simplesmente deletar e não reclamar, ignorando o spam, pode torná-lo conivente, pois o spammer continuará atuando tranqüilamente.

"Você se cadastrou em nosso site e, portanto, está recebendo esta mensagem. Caso queira sair de nossa lista de divulgação..."

Uma variação do tipo remove me. Alguns spams se utilizam dos recursos válidos de cadastro on-line de determinados sites para dar legitimidade ao e-mail. Novamente, não responda e reclame.

"Você foi indicado por um amigo e por isso estamos contatando-o. Caso queira sair de nossa lista de divulgação..."

Outra variação do tipo remove me... De fato, pode ser que você tenha sido indicado por um amigo. Neste caso, um amigo spammer ;-).

"De acordo com a lei xxxx, este e-mail não pode ser considerado spam..."
Uma das perguntas mais freqüentes sobre spam no ano passado foi com relação a esta suposta lei citada no final de vários spams. Não existe lei nem decreto que regulamente spam! Para maiores detalhes, consulte http://www.spambr.org/congresso.html.

"Consultamos sua home page, e sua empresa foi selecionada para participar de ... Esperamos não ter importunado com nosso contato..."

Decididamente, isto é spam.

Para todos os exemplos citados acima, siga os passos descritos na seção 6 deste artigo para garantir que providências sejam tomadas e que o spam não caia no esquecimento: reclame e exija providências.

5. Prevenção

Não existe uma receita milagrosa capaz de solucionar todos os problemas relacionados a spam. No entanto, alguns cuidados devem ser tomados pelo administrador da rede, enquanto outros devem ser tomados pelo usuário.

5.1 Recomendações ao administrador

Faz parte das atribuições do administrador da rede tratar os casos de spam originados ou destinados a rede sob sua responsabilidade. Assim, algumas recomendações imprescindíveis são fazer a configuração correta de seus servidores para não ser conivente com o envio de spam; cuidar das configurações capazes de reduzir o volume de spam recebido; educar os usuários sobre como lidar com spam e não ser spammer; etc, como discutidas abaixo.

Relay

Um servidor de correio eletrônico atua como relay quando ele processa um e-mail, sendo que nem o remetente, nem o destinatário são usuários do servidor em questão. Servidores de correio que permitem relay já foram usados na Internet de maneira válida. No entanto, atualmente, constituem uma ameaça na rede, pois são usados pelos spammers para disparar seus junk e-mails indiscriminadamente. O uso de servidores como relay permite aos spammers aumentar o envio destes e-mails, driblar filtros, despistar sua verdadeira identidade e sem pagar nada por isto!

As versões mais recentes do Sendmail são anti-relay. Caso você utilize outro servidor de correio, pesquise como fechar relays urgentemente.
O site http://www.abuse.net/relay.html permite testar se seu servidor está com relay aberto.

Filtros

Dentre as alternativas para filtrar e-mails indesejáveis, temos:
A definição de blackhole lists no SMTP server, como no Sendmail por exemplo. Com este recurso, o servidor rejeita os e-mails originados de potenciais redes ou usuários spammers, pré-definidos numa lista.
Pode-se definir filtros no cliente de e-mail também. Utilitários como o Eudora e o Pine, por exemplo, possuem esta funcionalidade. Alguns administradores questionam o uso de filtros na máquina do usuário final, argumentando que o spam já atingiu parte de seu objetivo, pois já desperdiçou recursos do servidor e banda do provedor. No entanto, ainda assim é uma alternativa a se considerar.

O grande problema com a utilização de filtros é o cuidado em não rejeitar e-mails válidos. Assim, use filtros em casos específicos e com a devida autorização da empresa. Imagine que, ao filtrar os e-mails de um domínio reconhecidamente spammer, o diretor geral da empresa deixou de receber e-mails de sua amante...

Listas da ORBs e MAPS

Existem duas entidades na Internet que mantêm bases de dados de servidores de e-mail que permitem relay: a ORBS (Open Relay Behaviour-modification System, www.orbs.org) e o MAPS (Mail Abuse Prevention System, http://www.mail-abuse.org).

Uma prática recomendada aos administradores é a configuração de seus servidores de e-mail para rejeitar e-mails originados das redes listadas nestas duas bases de dados. A experiência tem demonstrado que o uso deste recurso

reduz significativamente os problemas com spam e mailbombing através de spam/relay.

Para configuração do Sendmail neste caso, consulte: http://www.sendmail.org/tips/relaying.html

Educação e conscientização dos usuários

A educação continua sendo a melhor alternativa. Educar e conscientizar os usuários de sua rede sobre como lidar com spam: como reclamar, a quem recorrer, como não colaborar com spam na rede, por que não enviar spam, etc. As principais recomendações ao usuário estão comentadas na seção 5.2.

Spam e Políticas de segurança

As políticas de uso aceitável de sua rede, AUPs, devem ter normas claramente definidas para casos de spam, para que se tenha como advertir e até punir o usuário que não seguir as regras estabelecidas. Tais políticas devem prever desde advertências em caso de mau uso da conta de e-mail, até o cancelamento da mesma em casos recorrentes de spam enviados pelo mesmo usuário, por exemplo.

RFC 2142: abuse@domínio, postmaster@domínio, etc...

O RFC 2142, Mailbox Names for Common Services, Roles and Functions, recomenda os aliases básicos necessários para garantir a comunicação entre as inúmeras redes na Internet. Os principais aliases recomendados, relacionados com incidentes de segurança e abusos na rede são: abuse@domínio, security@domínio, postmaster@domínio e hostmaster@domínio. Todo bom administrador deve ter implementado os aliases mencionados, ler e responder as notificações recebidas através deles.

Envio de reclamações

Enviar reclamações, exigindo providências aos responsáveis pelo spam ou por uso de relay é, principalmente, tarefa do administrador. A seção 6 trata justamente de como reclamar.

5.2 Recomendações ao usuário

O número de usuários na Internet cresce assustadoramente a cada minuto, sendo que muitos estão aprendendo a viver ou sobreviver nesta "aldeia global". Assim, cabe ao administrador de rede conscientizar seus usuários sobre regras, dicas e cuidados que devem ser seguidos para melhor conviver no mundo virtual. Como agir diante do recebimento de spam, como não incentivar o surgimento de spam, ou ainda, cuidados para não se tornar um spammer, devem fazer parte deste treinamento dos usuários.

A seguir, são listados alguns conselhos básicos aos usuários:

Siga a Netiqueta

Embora a filosofia da Internet seja um tanto quanto anárquica, existem algumas regras básicas de bom comportamento na rede. Algo como as regras de boa educação para viver em sociedade: "por favor", "obrigado", "com licenç", "não gritar" e assim por diante. O RFC 1855, que trata da Netiqueta, pode parecer antigo por ser de 1995, mas ainda é muito adequado, principalmente com relação a comunicação por e-mail e WWW. Aos que não conhecem a Netiqueta, consulte as referências [3] e [5], além da Netiquette Home Page em http://wise.fau.edu/netiquette/netiquette.html.

Não repasse boatos ou correntes

Verifique sempre a veracidade de uma determinada mensagem antes de repassá-la. Na dúvida, não repasse. Existem casos de funcionários demitidos por justa causa e processados por repassarem boatos.

Quando decidir repassar mensagens deste tipo, mesmo após certificar-se da veracidade da mesma, restrinja ao máximo os destinatários e pense sempre se seus amigos estariam realmente interessados em receber tal informação: cuidado para não se transformar num spammer.

A regra básica é: fuja das correntes e fique atento aos boatos!

Não caia em "contos do vigário": remove me..., just delete..., etc.

Fique atento ao conteúdo dos spams recebidos e não seja ingênuo, não caia nos artifícios usados pelos spammers, como exemplificado na seção 4 deste artigo.

Nunca responda para um spammer, nem se envolva em discussões com o mesmo. Isto gera mais spam!

Ao receber um spam, entre em contato com os administradores de sua rede ou, se preferir reclamar diretamente, faça-o endereçando a notificação aos administradores da rede origem do spam, como mostrado na seção 6. Não responda ou tente reclamar diretamente ao spammer, caso seja possível identificá-lo no e-mail. Agindo desta maneira, você estará se envolvendo em discussões que não solucionarão o problema, podendo inclusive aumentá-lo. Afinal um spammer convicto poderá gerar algum esquema de retaliação que só fará piorar a situação.

Não tente revidar, atacando o spammer: este tipo de retaliação não funciona.

A idéia de "olho por olho, dente por dente" não se aplica neste contexto. Não tente revidar a perturbação ou até mesmo o ataque recebido de um spammer. Este tipo de atitude não é ética, não é recomendável e não vai resolver o problema. Se você decidir retaliar um spam, usando o mesmo método, lembre-se que estará se tornando um spammer. Além disto, existem várias maneiras de se forjar um e-mail de spam e, portanto, você está arriscado a retaliar o domínio errado. Finalmente, a retaliação estará atraindo mais atenção e publicidade para o spammer: tudo o que ele mais queria!

Cuidados de higiene com seu(s) e-mail(s)

Evite se cadastrar em sites que prometem não divulgar seus dados. Evite se cadastrar em vários sites e listas de divulgação de atualizações de informação, etc. Caso sua postura pessoal seja de um internauta ávido por informações e que gosta de receber malas diretas, divulgação de sites, etc, então, uma prática recomendada e muito utilizada é manter contas de e-mail separadas para seus interesses pessoais, fora do ambiente do trabalho, isto pode não solucionar o problema, mas ajuda a minimizá-lo. Tenho amigos que dizem: "Ah! Nas minhas navegações pela rede, só uso a minha conta <fulano@provedor_X>: ela é para os spams!"

Filtros

Alguns programas clientes de e-mail apresentam funcionalidades que permitem filtrar e-mails de spam. Novamente, tais funcionalidades não resolvem todos os problemas, mas podem driblar um pouco a questão, diminuindo o volume de junk e-mails em sua caixa postal. Lembre-se sempre de relatar ao administrador de sua rede o recebimento de spams, ele poderá incrementar a política de defesa contra spam da rede como um todo.

6. Como agir diante de um spam?

O mandamento básico é reclamar. Não se deve ignorar o recebimento de spam, pois isto encoraja cada vez mais este tipo de prática.

Em se tratando do usuário final, recomenda-se contatar o administrador de sua rede, notificando o spam, enviando o e-mail recebido com o header completo. Caso o usuário final decida reclamar ele próprio, então deve seguir as orientações abaixo.

Com relação ao administrador de rede, é responsabilidade deste reclamar dos spams recebidos pelos usuários, assim como tomar providências em caso de uso de seu servidor de e-mail como relay ou ainda, em casos de spams enviados por usuários de sua rede.

Para reclamar de um spam recebido, deve-se:

- Enviar a notificação ao administrador ou contato técnico pela rede origem do spam; nunca diretamente ao spammer! A notificação deve ser enviada também para abuse@dominio_spammer e para os grupos de segurança responsáveis pelas redes vítima e spammer;
- Anexar à reclamação, o header completo do e-mail de spam. O header é a peça principal a ser investigada num spam, analise-o cuidadosamente, identificando a rede origem e eventuais servidores usados como relay. Esta é a parte mais complicada, pois o header de spam não é confiável e pode ter sido forjado em vários níveis. Algumas dicas sobre análise de header:
    - Desconfie dos campos FROM: e TO:. Eles podem conter usuários inválidos, domínios inválidos ou "spoofados", isto é, os domínios usados no FROM: e no TO: podem ser inexistentes, ou ainda não serem, de fato, a origem do spam. Este recurso é usado para confundir e distrair a atenção do administrador ao tentar identificar a origem do spam, ou em outros casos para difamar o domínio "spoofado";
    - Examine todos os números IP e domínios que aparecem no header, tente resolvê-los pelo DNS;

    - Estude, detalhadamente. Se conhecer a sintaxe dos headers gerados, maiores serão as chances de sucesso no processo de análise de headers de spam;
    - Cuidado com ferramentas de análise automática de headers, elas podem gerar resultados falsos e originar reclamações incoerentes.
- Anexar à reclamação, o conteúdo da mensagem de spam, somente se incluir informações relevantes para uma eventual investigação;
- Em caso de uso de relay, deve-se copiar a reclamação para o administrador ou contato técnico pela rede que hospeda o servidor usado como relay, para abuse@domínio_relay e para o grupo de segurança responsável pela rede em questão;
- Opcionalmente, pode-se encaminhar a reclamação com cópia para o MAPS através do e-mail relays@mail-abuse.org, incluindo, no corpo da mensagem, a diretiva: Relay:<IP-do-servidor-com-relay>, este procedimento é um tipo de denúncia automática.

Se o administrador receber denúncias de spam partindo de sua rede, as recomendações são:

- Identificar o usuário que enviou o spam;
- Advertir ou punir o usuário spammer de acordo com as AUPs;
- Responder ao reclamante.

Por outro lado, caso a notificação seja de uso do servidor de e-mail como relay, o administrador deve tomar as providências para corrigir o problema o mais rápido possível, sob pena de ser conivente com o envio de spam, enquanto não solucionar a questão e responder aos reclamantes. No caso de notificação recebida da ORBs, é necessário ainda solicitar a remoção do número IP do servidor da base mantida pela entidade.

7. Conclusão

O volume de spam na Internet tem aumentado assustadoramente, e isto tem preocupado usuários e administradores. O repúdio ao spam na rede não surge gratuitamente, mas sim graças a fatores como: a perturbação, chateação e mau humor das vítimas; o prejuízo causado com o desperdício de recursos que vão, desde o tempo gasto pelos milhões de internautas em limpar suas caixas postais todos os dias, até o tempo gasto pelos administradores, grupos de combate ao spam e grupos de segurança em tentar de alguma maneira coibir tal ato, culminando no desperdício e até degradação de desempenho de servidores e da rede.

Aos leitores que se interessam pelo tema, recomenda-se consultar os sites de entidades reconhecidas pelo combate ao spam: ORBS, MAPS, CAUCE, CAUBE, SpamCop, Abuse.net e Movimento Brasileiro de Combate ao spam.

É difícil encarar com otimismo o panorama apresentado na Internet hoje com relação ao problema de spam. Para diminuir o problema cabe a cada um colaborar: não se omitindo, não sendo conivente, reclamando, exigindo providências, se prevenindo para evitar que os spams invadam definitivamente sua caixa postal e a Internet de modo geral.

8. Sites relacionados

Abuse.net Home Page: http://www.abuse.net

CAUBE – Coalition Against Unsolicited Bulk E-mail,

Australia: http://www.caube.org.au

CAUCE – Coalition Against Unsolicited Commercial E-mail: http://www.cauce.org

CIAC Hoaxbusters Home Page: http://hoaxbusters.ciac.org

Computer Virus Myths: http://www.Vyths.com

Fight Spam on the Internet: http://spam.abuse.net

MAPS - Mail Abuse Prevention System: http://www.mail-abuse.org

Mike's Anti-spam Page: http://www.zip.com.au/~mfleming/antispam

Movimento Brasileiro de Combate ao spam: http://www.spambr.org

Netiquette Home Page: http://wise.fau.edu/netiquette/netiquette.html

ORBS - Open Relay Behaviour-modification System: http://www.orbs.org

Sendmail Home Page: http://www.sendmail.org

SpamCop: http://spamcop.net

spam Laws, David E. Sorkin: http://www.spamlaws.com

Referências bibliográficas

[1] Allowing controlled SMTP relaying in

Sendmail: http://www.sendmail.org/tips/relaying.html

[2] Anti-Relay: Stop Third-Party Mail Relay: http://maps.vix.com/tsi

[3] Diretrizes da Netiqueta – Tradução de José Carlos da

Silva; http://www.allnet.com.br/freedom/netqueta.htm

[4] Mail Relay Testing: http://www.abuse.net/relay.html

[5] Anti-Relay: Stop Third-Party Mail Relay: http://maps.vix.com/tsi

[6] RFC 1855; Hambridge, S.; Netiquete Guidelines;

1995: http://www.ietf.rnp.br/ftp/rfc/rfc1855.txt

[7] RFC 2142; Crocker, D. ; Mailbox Names for Common Services, Roles and

Functions; 1997:http://www.ietf.rnp.br/ftp/rfc/rfc2142.txt

[8] RFC 2505; Lindberg, G.; Anti-Spam Recommendations for SMTP MTAs;

1999: http://www.ietf.rnp.br/ftp/rfc/rfc2505.txt

[9] Stop SPAM FAQ: http://www.mall-net.com/spamfaq.html

NewsGeneration, um serviço oferecido pela RNP – Rede Nacional de Ensino e Pesquisa