



Comitê Gestor da Internet no Brasil

Cartilha de Segurança para Internet

Parte VI: *Spam*



Versão 3.1
2006

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte VI: *Spam*

Esta parte da Cartilha aborda o conceito de *spam* e os problemas que ele pode acarretar para usuários, provedores e empresas. Também são citadas técnicas de filtragem que podem ser utilizadas por usuários para tentar bloquear o recebimento de *spams*.

Sumário

1	<i>Spam</i>	3
1.1	Quais são os problemas que o <i>spam</i> pode causar para um usuário da Internet?	3
1.2	Quais são os problemas que o <i>spam</i> pode causar para os provedores de acesso, <i>backbones</i> e empresas?	3
1.3	Como os <i>spammers</i> conseguem endereços de <i>e-mail</i> ?	4
1.4	Como os <i>spammers</i> confirmam que um endereço de <i>e-mail</i> existe?	4
1.5	Como fazer para filtrar os <i>e-mails</i> de modo a barrar o recebimento de <i>spams</i> ?	5
1.6	Para quem devo reclamar quando receber um <i>spam</i> ?	6
1.7	Que informações devo incluir numa reclamação de <i>spam</i> ?	6
1.8	O que devo fazer ao identificar em um <i>spam</i> um caso de <i>phishing/scam</i> ?	7
1.9	Onde posso encontrar outras informações sobre <i>spam</i> ?	7
	Como Obter este Documento	8
	Licença de Uso da Cartilha	8
	Agradecimentos	8

1 Spam

Spam é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial E-mail*).

1.1 Quais são os problemas que o *spam* pode causar para um usuário da Internet?

Os usuários do serviço de correio eletrônico podem ser afetados de diversas formas. Alguns exemplos são:

Não recebimento de *e-mails*. Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de *spams* recebidos seja muito grande o usuário corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, o usuário não conseguirá mais receber *e-mails* e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. O usuário também pode deixar de receber *e-mails* em casos onde estejam sendo utilizadas regras anti-*spam* ineficientes, por exemplo, classificando como *spam* mensagens legítimas.

Gasto desnecessário de tempo. Para cada *spam* recebido, o usuário necessita gastar um determinado tempo para ler, identificar o *e-mail* como *spam* e removê-lo da caixa postal.

Aumento de custos. Independentemente do tipo de acesso a Internet utilizado, quem paga a conta pelo envio do *spam* é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado a Internet, cada *spam* representa alguns segundos a mais de ligação que ele estará pagando.

Perda de produtividade. Para quem utiliza o *e-mail* como uma ferramenta de trabalho, o recebimento de *spams* aumenta o tempo dedicado à tarefa de leitura de *e-mails*, além de existir a chance de mensagens importantes não serem lidas, serem lidas com atraso ou apagadas por engano.

Conteúdo impróprio ou ofensivo. Como a maior parte dos *spams* são enviados para conjuntos aleatórios de endereços de *e-mail*, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

Prejuízos financeiros causados por fraude. O *spam* tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros. Este tipo de *spam* é conhecido como *phishing/scam* (maiores detalhes na [Parte IV: Fraudes na Internet](#)). O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas neste tipo de mensagem fraudulenta.

1.2 Quais são os problemas que o *spam* pode causar para os provedores de acesso, *backbones* e empresas?

Para as empresas e provedores os problemas são inúmeros e, muitas vezes, o custo adicional causado pelo *spam* é transferido para a conta a ser paga pelos usuários.

Alguns dos problemas sentidos pelos provedores e empresas são:

Impacto na banda. Para as empresas e provedores o volume de tráfego gerado por causa de *spams* os obriga a aumentar a capacidade de seus *links* de conexão com a Internet. Como o custo dos *links* é alto, isto diminui os lucros do provedor e muitas vezes pode refletir no aumento dos custos para o usuário.

Má utilização dos servidores. Os servidores de *e-mail* dedicam boa parte do seu tempo de processamento para tratar das mensagens não solicitadas. Além disso, o espaço em disco ocupado por mensagens não solicitadas enviadas para um grande número de usuários é considerável.

Inclusão em listas de bloqueio. O provedor que tenha usuários envolvidos em casos de *spam* pode ter sua rede incluída em listas de bloqueio. Esta inclusão pode prejudicar o recebimento de *e-mails* por parte de seus usuários e ocasionar a perda de clientes.

Investimento em pessoal e equipamentos. Para lidar com todos os problemas gerados pelo *spam*, os provedores necessitam contratar mais técnicos especializados, comprar equipamentos e acrescentar sistemas de filtragem de *spam*. Como consequência os custos do provedor aumentam.

1.3 Como os *spammers* conseguem endereços de *e-mail*?

Os *spammers* utilizam diversas formas para obter endereços de *e-mail*, desde a compra de bancos de dados com *e-mails* variados, até a produção de suas próprias listas de *e-mails* obtidos via programas maliciosos, *harvesting* e ataques de dicionário.

A obtenção através de programas maliciosos é possível devido à grande ligação entre os *spammers* e aqueles que desenvolvem estes programas. Um programa malicioso, muitas vezes, é projetado também para varrer o computador onde foi instalado em busca de endereços de *e-mail*, por exemplo, na lista de endereços (*address book*) do usuário. Os endereços de *e-mail* coletados são, então, repassados para os *spammers*.

Já o *harvesting* é uma técnica utilizada por *spammers* que consiste em varrer páginas *Web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

Muitas vezes, os endereços de *e-mail* aparecem de forma ofuscada. Exemplos são as páginas *Web* ou listas de discussão que apresentam os endereços de *e-mail* com o “@” substituído por “(at)” e os pontos substituídos pela palavra “dot”. Vale lembrar, entretanto, que os programas que implementam as técnicas de *harvesting* utilizadas pelos *spammers* podem prever estas substituições.

Nos ataques de dicionário, por sua vez, o *spammer* forma endereços de *e-mail* a partir de listas de nomes de pessoas, de palavras presentes em dicionários e/ou da combinação de caracteres alfanuméricos.

1.4 Como os *spammers* confirmam que um endereço de *e-mail* existe?

Os *spammers* utilizam vários artifícios para confirmar a existência de endereços de *e-mail*. Um destes artifícios consiste em enviar mensagens para os endereços formados em ataques de dicionários

e, com base nas respostas enviadas pelo servidores de *e-mail* que receberam as mensagens, identificar quais endereços são válidos e quais não são.

Outro artifício largamente utilizado é a inclusão no *spam* de um suposto mecanismo para a remoção da lista de *e-mails*, que pode ser um *link* ou endereço de *e-mail*. Ao receberem uma solicitação de remoção, os *spammers* confirmam que o endereço de *e-mail* é válido e realmente alguém o utiliza.

Uma outra forma para verificar endereços é o *Web bug*. *Web bug* é uma imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esta página *Web* ou mensagem de *e-mail*.

Quando o *Web bug* é visualizado, diversas informações são armazenadas no servidor onde está hospedado, tais como: o endereço IP do computador que o acessou, a URL completa da imagem que corresponde ao *Web bug*, o horário em que foi visualizado, etc.

Por exemplo, um *spammer* poderia utilizar *Web bugs* para a validação de endereços de *e-mail* da seguinte forma:

- criando a imagem do *Web bug* com o nome do endereço de *e-mail* que quer validar;
Exemplo: fulano.png
- hospedando o *Web bug* em um servidor onde tenha acesso a informações que serão geradas quando o *Web bug* for visualizado;
- criando uma mensagem de *e-mail* no formato HTML, que tenha em seu conteúdo a URL completa da imagem correspondente ao *Web bug*;
Exemplo: <http://www.dominio-do-spammer.example.org/fulano.png>
- enviando a mensagem criada para o endereço de *e-mail* a ser validado.
Exemplo: fulano@dominio-do-fulano.example.org

Quando o usuário “fulano” abre a mensagem enviada pelo *spammer* em seu programa leitor de *e-mails*, o *Web bug* é acessado e o *spammer* tem a confirmação de que o endereço de *e-mail* do “fulano” é válido.

Para impedir que este artifício tenha sucesso e evitar que um endereço de *e-mail* seja validado por um *spammer*, é possível desabilitar no programa leitor de *e-mails* o modo de visualização no formato HTML.

1.5 Como fazer para filtrar os *e-mails* de modo a barrar o recebimento de *spams*?

Existem basicamente dois tipos de *software* que podem ser utilizados para barrar *spams*: aqueles que são colocados nos servidores, e que filtram os *e-mails* antes que cheguem até o usuário, e aqueles que são instalados nos computadores dos usuários, que filtram os *e-mails* com base em regras individuais de cada usuário.

Podem ser encontradas referências para diversas ferramentas de filtragem de *e-mails* nas páginas abaixo:

- *Spam e-mail blocking and filtering* – <http://spam.abuse.net/userhelp/#filter>
- *Anti Spam Yellow Pages* – <http://www.antispamyellowpages.com/>

Também é interessante consultar seu provedor de acesso, ou o administrador de sua rede, para verificar se existe algum recurso anti-*spam* disponível e como utilizá-lo.

1.6 Para quem devo reclamar quando receber um *spam*?

Deve-se reclamar de *spams* para os responsáveis pela rede de onde partiu a mensagem. Se esta rede possuir uma política de uso aceitável, a pessoa que enviou o *spam* pode receber as penalidades que nela estão previstas.

Muitas vezes, porém, é difícil conhecer a real origem do *spam*. Os *spammers* costumam enviar suas mensagens através de máquinas mal configuradas, que permitem que terceiros as utilizem para enviar os *e-mails*. Se isto ocorrer, a reclamação para a rede de origem do *spam* servirá para alertar os seus responsáveis dos problemas com suas máquinas.

Além de enviar a reclamação para os responsáveis pela rede de onde saiu a mensagem, procure manter o *e-mail* mail-abuse@cert.br na cópia de reclamações de *spam*. Deste modo, o CERT.br pode manter dados estatísticos sobre a incidência e origem de *spams* no Brasil e, também, identificar máquinas mal configuradas que estejam sendo abusadas por *spammers*.

Vale comentar que recomenda-se não responder a um *spam* ou enviar uma mensagem solicitando a remoção da lista de *e-mails*. Geralmente, este é um dos métodos que os *spammers* utilizam para confirmar que um endereço de *e-mail* é válido e realmente alguém o utiliza.

Informações sobre como encontrar os responsáveis por uma rede são apresentadas na [Parte VII: Incidentes de Segurança e Uso Abusivo da Rede](#).

1.7 Que informações devo incluir numa reclamação de *spam*?

Para que os responsáveis por uma rede possam identificar a origem de um *spam* é necessário que seja enviada a mensagem recebida acompanhada do seu **cabeçalho completo** (*header*).

É no cabeçalho de uma mensagem que estão as informações sobre o endereço IP de origem da mensagem, por quais servidores de *e-mail* a mensagem passou, entre outras.

Informações sobre como obter os cabeçalhos de mensagens podem ser encontradas em <http://www.antispam.org.br/header.html>.

Informações sobre como entender os diversos campos normalmente encontrados nos cabeçalhos de *e-mails* estão disponíveis nas páginas abaixo (em inglês):

- *Reading Email Headers* – <http://www.stopspam.org/email/headers.html>
- *Tracking Spam* – <http://www.claws-and-paws.com/spam-1/tracking.html>

1.8 O que devo fazer ao identificar em um *spam* um caso de *phishing/scam*?

Ao identificar um *spam* como sendo um caso de *phishing/scam*, você deve enviar uma reclamação para os responsáveis pela rede de onde partiu a mensagem e para os responsáveis pelo *site* onde o esquema fraudulento está sendo hospedado¹. A reclamação deve conter não só o cabeçalho (como visto na seção 1.7), mas também o **conteúdo completo** da mensagem recebida.

Dicas sobre como obter o conteúdo completo de mensagens em diversos programas leitores de *e-mails* estão disponíveis em <http://www.spamcop.net/fom-serve/cache/19.html> (em inglês).

Além de enviar a reclamação para os responsáveis pela rede de onde saiu a mensagem e pelo *site* onde o esquema fraudulento está sendo hospedado, procure manter o *e-mail* cert@cert.br na cópia da reclamação. Deste modo, o CERT.br pode manter dados estatísticos sobre a incidência e origem de fraudes no Brasil e, também, repassar a reclamação para os contatos dos responsáveis que, por ventura, não tenham sido identificados.

É muito importante incluir o conteúdo completo da mensagem na reclamação, pois só assim será possível identificar o *site* utilizado para hospedar o esquema fraudulento, que pode ser uma página clonada de uma instituição financeira, um arquivo malicioso para furtar dados pessoais e financeiros de usuários, entre outros.

Mais detalhes sobre *phishing/scam* e outros tipos de fraude via Internet podem ser encontrados na [Parte IV: Fraudes na Internet](#).

1.9 Onde posso encontrar outras informações sobre *spam*?

Diversas informações podem ser encontradas no *site* <http://www.antispam.br/>, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), e que constitui uma fonte de referência sobre o *spam*. Este *site* tem o compromisso de informar o usuário e o administrador de redes sobre o *spam*, suas implicações e formas de proteção e combate.

¹Informações sobre como obter contatos dos responsáveis de uma rede estão na [Parte VII: Incidentes de Segurança e Uso Abusivo da Rede](#).

Como Obter este Documento

Este documento pode ser obtido em <http://cartilha.cert.br/>. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Licença de Uso da Cartilha

Este documento é Copyright © 2000–2006 CERT.br. Ele pode ser livremente distribuído desde que sejam respeitadas as seguintes condições:

1. É permitido fazer e distribuir gratuitamente cópias impressas inalteradas deste documento, acompanhado desta Licença de Uso e de instruções de como obtê-lo através da Internet.
2. É permitido fazer *links* para a página <http://cartilha.cert.br/>, ou para páginas dentro deste *site* que contenham partes específicas da Cartilha.
3. Para reprodução do documento, completo ou em partes, como parte de *site* ou de outro tipo de material, deve ser assinado um Termo de Licença de Uso, e a autoria deve ser citada da seguinte forma: “Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em <http://cartilha.cert.br/>.”
4. É vedada a exibição ou a distribuição total ou parcial de versões modificadas deste documento, a produção de material derivado sem expressa autorização do CERT.br, bem como a comercialização no todo ou em parte de cópias do referido documento.

Informações sobre o Termo de Licença de Uso podem ser solicitadas para doc@cert.br. Embora todos os cuidados tenham sido tomados na preparação deste documento, o CERT.br não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais consequências que possam advir do seu uso.

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.