Diversas bases de dados acessíveis ao público indicam que o seguinte endereço IP, [inserir número], pode ser um servidor de correio eletrônico aberto ("open relay mail server") ou um servidor *proxy* aberto ("open proxy server"). Ademais, os indícios são de que seu servidor utiliza este endereço IP. Esta carta contém importante informação que pode afetar a presença de sua empresa na Internet.

Este *e-mail* é enviado como parte da "Operation Secure Your Server" (Operação para a Segurança de seu Servidor), um projeto conjunto da "Federal Trade Commission" dos Estados Unidos e Organizações Governamentais de outros países, preocupados com os problemas advindos da proliferação do fenômeno do "spam" – mensagem comercial não solicitada. O projeto pretende orientar as empresas a respeito da segurança dos servidores para que possam evitar que seus servidores se transformem em uma fonte inesperada de mensagens não solicitadas. Como primeira medida, a sugestão é para que feche seu servidor de correio eletrônico aberto ("open relay server") ou seu servidor *proxy* aberto ("open proxy server").

"Open relays" e "open proxies" são servidores que permitem a qualquer microcomputador do mundo enviar mensagens eletrônicas por meio deles para outros endereços eletrônicos. Estes servidores são, com freqüência, explorados por pessoas que inundam a Internet com mensagens comerciais não solicitadas, conhecidas em inglês como "spam". Este abuso cria problemas, de âmbito internacional, aos consumidores, às autoridades aplicadoras da lei, e, até mesmo, à sua própria empresa. Por exemplo, pode ocorrer que os destinatários do "spam" tenham a impressão de que o "spam" venha de seu sistema; seus servidores e seus recursos de serviços de Internet podem ser utilizados por terceiros desconhecidos; suas conexões de Rede podem entrar em colapso com o tráfego; seus custos administrativos podem aumentar; ou seu Serviço de Provedor de Internet pode cancelar seu acesso à Internet. Dotar seus servidores de segurança ajudará a proteger seu sistema de vir a ser usado por usuários indevidos.

Para mais informações sobre "open relays", "open proxies" e sobre como proteger sua organização dos problemas associados a estes servidores abertos e inseguros, incluindo instruções passo a passo sobre como fechá-los, favor acessar em www.ftc.gov/secureyourserver uma Página Especializada, que inclui uma lista das agências participantes deste projeto. Para acesso direto às instruções sobre como fechar seu "open relay" ou "open proxy", acesse www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.htm.

Caso tenha dúvidas sobre as instruções ou esta carta, por favor escreva para secureyourserver@ftc.gov.