

Autenticação aprimorada

Para os remetentes de email, a publicação de um registro do SPF fornece um valor comercial considerável, por proteger seus nomes de domínio e suas marcas. Para os destinatários, a autenticação de entrada fornece um nível adicional de detecção aprimorada de spams e phishings para proteger as organizações e seus funcionários. Organizações de todo o mundo já estão integrando a identificação do remetente em suas soluções anti-spam em camadas. Hoje, mais de uma dezena de fornecedores líderes de MTAs SMTP e de soluções de código-fonte aberto, incluindo a Sendmail, oferecem essa funcionalidade. Ao incluir o resultado da identificação do remetente à heurística existente e aplicar a reputação de domínio, as redes de recebimento obtêm um nível mais alto de detecção de spams e phishings com menos falsos positivos, o que resulta em uma maior confiança online dos funcionários. A autenticação de entrada oferece a seus funcionários uma proteção adicional contra emails enganosos, reduzindo o risco de explorações direcionadas tanto às suas informações pessoais quanto aos dados corporativos.

Adoção mundial

Hoje, mais de 2,5 milhões de empresas já possuem registros do SPF publicados, e mais de 600 milhões de usuários estão protegidos pelo SIDF. Essa adoção mundial está aumentando consideravelmente a precisão da filtragem de emails para garantir a proteção contra explorações por spams e phishings. Para dar suporte a todos os segmentos de clientes, do consumidor final aos ambientes empresariais, a Microsoft integrou o SIDF ao Microsoft® Exchange Server 2003 Service Pack 2 (SP2), ao Microsoft Exchange Hosted Filtering, ao serviço de emails baseado na Web do Microsoft Hotmail®, ao Microsoft Windows® Live Mail, ao Microsoft Outlook® Express e ao cliente de mensagens e colaboração do Outlook. Com a implementação da identificação do remetente, as organizações ajudarão a aumentar a confiança online, gerando uma vantagem competitiva para suas iniciativas de estabelecimento de marca e de marketing online. Outras soluções líderes da indústria estão disponíveis em:



Para obter mais informações sobre o SIDF, incluindo ferramentas, recursos e soluções de terceiros, visite www.microsoft.com/senderid (em inglês). Para obter informações sobre o compromisso da Microsoft com a segurança online, incluindo colaboração da indústria, imposição, treinamento para clientes e tecnologias inovadoras, visite www.microsoft.com/safety (em inglês).

© 2006 Microsoft Corporation. Todos os direitos reservados.

Este documento destina-se apenas a fins informativos. A MICROSOFT NÃO FORNECE GARANTIAS, EXPRESSAS OU IMPLÍCITAS, NESTE RESUMO. Microsoft, Hotmail, Outlook e Windows são marcas registradas ou marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países. Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

0406

Microsoft



Sender ID Framework

Recuperando a confiança no email

Identifique spams e detecte phishings

Microsoft

www.microsoft.com/senderid

Sender ID Framework

O que é a identificação do remetente?

Uma peça importante da infra-estrutura comercial crítica, o email permite comunicações confiáveis com clientes e parceiros, relações comerciais globais, comércio eletrônico e transações bancárias online. Infelizmente, os remetentes de spam e phishing continuam explorando essa infra-estrutura, criando riscos de segurança para os usuários e ameaçando marcas e domínios de empresas em todo o mundo.

Trabalhando com líderes da indústria, ISPs e fornecedores de sistemas de email, a Microsoft está patrocinando o SIDF (Sender ID Framework) como uma solução líder de autenticação de emails para a identificação de spams, a detecção de phishings e o aumento da segurança online.

Fácil de implementar e implantar — por um preço baixo

O SIDF é usado para validar a identidade de um remetente a fim de ajudar a detectar e reduzir a exploração por spams e phishings antes que eles cheguem à caixa de entrada do usuário. Ele verifica se cada mensagem de email é realmente originada do domínio da Internet do qual afirma ser, aumentando assim a confiança do cliente e protegendo a reputação online de todos os remetentes, incluindo empresas de todos os portes e mercados verticais. O SIDF também pode proteger instituições financeiras, sites de comércio eletrônico e outras organizações globais.

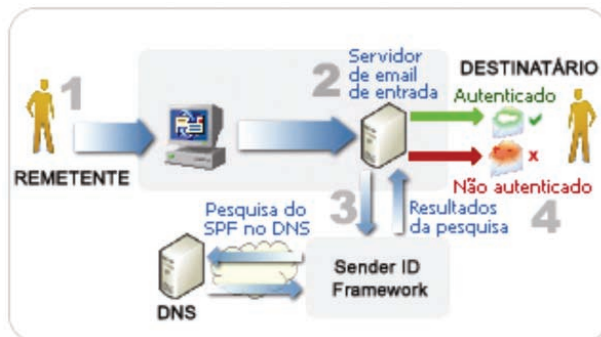
Ele combina as tecnologias SPF (Sender Policy Framework) e Microsoft CallerID for E-mail a fim de oferecer uma solução de autenticação integrada e de baixo custo que seja fácil de implantar e manter. Com a integração do SIDF, você pode:

- Aumentar a capacidade de entrega de emails legítimos.
- Reduzir os falsos positivos.
- Aumentar a satisfação e a confiança dos clientes.
- Reduzir a exposição dos clientes às tentativas de phishing.
- Proteger a reputação da marca da sua organização contra falsificações.
- Criar e associar a reputação da marca da sua organização a correspondências conhecidas.
- Aumentar sua capacidade de bloquear remetentes de spam conhecidos.

Como funciona a identificação do remetente

Seu administrador de domínio, postmaster ou provedor de hospedagem precisa criar e publicar um registro do SPF que identifique os endereços IP dos seus servidores de email de saída. Esse registro de texto simples é inserido, ou publicado, no arquivo de zona de DNS (Sistema de Nome de Domínio) do seu domínio.

Em um processo de autenticação que é transparente para o remetente e o destinatário, o SIDF usa esse registro para verificar se cada mensagem é de uma origem autorizada. Não é necessário nenhum software cliente adicional, o que significa que os usuários podem enviar e receber emails da mesma maneira como fazem hoje. O gráfico a seguir descreve o processo de verificação.



1. O remetente envia uma mensagem de email.
2. O servidor de email de entrada do destinatário recebe a mensagem.
3. O servidor de email de entrada verifica o domínio de origem e o DNS do registro do SPF. Ele, então, determina se o endereço IP do servidor de email de saída corresponde a um endereço IP do registro do SPF.
4. Os filtros de spam revisam os resultados e os combinam à heurística anti-spam existente para determinar se a mensagem deve ser entregue na caixa de entrada do usuário ou na pasta de emails indesejados, ou se ela deve ser excluída. Os filtros também podem usar o resultado da identificação do remetente para avaliar a reputação do remetente como uma heurística adicional, aprimorando a detecção de spams.

Criando um registro do SPF

A primeira etapa de uma implantação bem-sucedida do SIDF é a criação de um registro do SPF, que lista os endereços IP dos servidores que enviam mensagens de email em nome de sua organização. Como as empresas geralmente dependem de terceiros para ter serviços de email e comércio, essas partes devem ser incluídas no registro do SPF. O registro deve incluir qualquer pessoa que contate clientes em sua organização, como dos setores de marketing direto, suporte terceirizado a clientes ou relacionamentos com investidores, propaganda, remessa e outros.

Após identificar esses remetentes, você precisa incluir os endereços IP de seus servidores de email de saída em seu registro do SPF. Você pode listá-los explicitamente ou, para ter mais flexibilidade e conveniência, pode apontar para seus registros do SPF publicados a partir do registro do SPF. Depois de fazer isso, e depois de publicar o registro do SPF no DNS, você pode enviar emails normalmente, sem nenhuma interrupção do serviço ou impacto nos MTAs (Agentes de Transferência de Mensagens) de saída. Para garantir que o registro do SPF esteja atualizado, recomendamos fazer uma revisão mensal dos endereços IP externos e internos.

Microsoft Sender ID SPF Record Wizard

Para ajudá-lo a criar um registro do SPF, o Microsoft Sender ID Framework SPF Record Wizard oferece um guia passo a passo simples. Esse guia, que possui quatro etapas, ajuda a identificar um domínio, exibir os registros publicados desse domínio, adicionar endereços IP e designar uma sintaxe de registro específica para redes de recebimento. Para obter mais informações, visite www.microsoft.com/senderid e clique em Resources (em inglês).



Sender ID