SPF e DKIM: o guia para reconhecer emails falsos

Autore: Francesco Zinghinì | **Data:** 25 Dicembre 2025

Todos os dias, a nossa caixa de correio é um vaivém de comunicações, um pouco como a praça de uma aldeia durante o mercado semanal. Há mensagens de trabalho, newsletters nas quais estamos inscritos e comunicações pessoais. No meio deste fluxo, porém, escondem-se também mensagens enganosas, tentativas de burla conhecidas como phishing. Como podemos distinguir um remetente fiável de um impostor? A resposta reside em três siglas de aspeto técnico, mas de funcionamento intuitivo: **SPF, DKIM** e DMARC. Imaginemo-las como documentos de identidade digitais que permitem verificar a autenticidade de quem nos escreve, unindo a tradição da confiança a uma inovação tecnológica indispensável para a nossa segurança.

Estes protocolos não são conceitos abstratos apenas para especialistas. Pelo contrário, representam a primeira linha de defesa contra as fraudes informáticas. Compreender o seu funcionamento significa dotar-se das ferramentas para navegar com maior consciência no mundo digital. Este artigo nasce com o objetivo de traduzir estes termos técnicos para uma linguagem simples e direta, para ajudar qualquer pessoa, independentemente das suas competências informáticas, a proteger a sua vida digital. Aprenderemos juntos a reconhecer os sinais de um email suspeito, transformando a nossa caixa de correio num lugar mais seguro.

Porque a confiança no email é como um aperto de mão

Na cultura mediterrânica, um aperto de mão sempre selou um acordo, representando um pacto de confiança. No mundo digital, esta confiança é igualmente fundamental, mas muito mais frágil. O perigo mais comum é o *spoofing*, uma técnica com a qual um mal-intencionado falsifica o endereço do remetente para fazer parecer que o email provém de uma fonte fidedigna, como o nosso banco, uma transportadora ou até mesmo um colega. O objetivo é quase sempre levar-nos a realizar ações prejudiciais, como revelar palavras-passe ou dados financeiros. Esta ameaça está longe de ser rara; aliás, é uma das principais causas de incidentes informáticos.

Os dados confirmam a gravidade do problema. Segundo o relatório Clusit 2024, em Itália os ataques informáticos aumentaram 65% em relação ao ano anterior, e o phishing representa uma das técnicas mais difundidas. Esta estatística alarmante destaca como a capacidade de verificar a identidade do remetente já não é uma opção, mas uma necessidade. Tal como não abriria a porta de casa a um estranho, é fundamental aprender a não “abrir” emails de remetentes não verificados. Os protocolos de autenticação como SPF e DKIM são as ferramentas que nos permitem fazer exatamente isso: controlar quem bate à nossa porta digital.

SPF: o controlador de passaportes digitais

O protocolo **SPF (Sender Policy Framework)** pode ser imaginado como um rigoroso controlador de passaportes na fronteira digital. Em termos simples, o proprietário de um domínio (por exemplo, `omeubanco.pt`) publica uma lista oficial de “carteiros” autorizados, ou seja, os servidores de correio que têm

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

permissão para enviar emails em seu nome. Esta lista é pública e registada no sistema de nomes de domínio (DNS), uma espécie de lista telefónica da Internet. Quando recebemos um email, o nosso fornecedor de correio (como Gmail ou Outlook) verifica o endereço IP do servidor que o enviou e compara-o com a lista autorizada pelo domínio do remetente.

Se o endereço IP do servidor remetente estiver presente na lista SPF, o "passaporte" é carimbado e o email é considerado legítimo. Caso contrário, o servidor de correio etiqueta-o como suspeito, sinalizando-o ou, em alguns casos, bloqueando-o antes mesmo que chegue à nossa caixa de entrada. Este mecanismo é uma primeira e fundamental barreira contra o spoofing. Impede que um burlão use um servidor não autorizado para enviar emails fingindo ser o nosso banco, porque o seu "passaporte digital" resultaria imediatamente inválido. É um sistema baseado na transparência e na verificação, um pilar para construir um ambiente de email mais seguro.

DKIM: o selo de cera na era digital

Se o SPF controla quem pode enviar uma mensagem, o **DKIM (DomainKeys Identified Mail)** atua como um selo de cera numa carta antiga, garantindo a sua autenticidade e integridade. Este protocolo adiciona uma assinatura digital única ao cabeçalho de cada email enviado. A assinatura é criada utilizando uma chave privada, secreta e conhecida apenas pelo servidor do remetente. A chave pública correspondente, por outro lado, é acessível a todos através dos registos DNS do domínio, tal como a lista SPF. Quando o email chega ao destino, o servidor do destinatário utiliza a chave pública para verificar a assinatura digital.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Se a verificação for bem-sucedida, significa duas coisas fundamentais. Primeiro, o email provém efetivamente do domínio declarado, uma vez que apenas o legítimo proprietário possui a chave privada para criar aquela assinatura específica. Segundo, o conteúdo da mensagem não foi alterado durante o trajeto. Qualquer modificação, mesmo mínima, invalidaria a assinatura, tal como um selo de cera quebrado revelaria que a carta foi aberta. O DKIM, portanto, não só autentica o remetente, mas também protege a integridade da mensagem, assegurando-nos que o que lemos é exatamente o que foi escrito, sem adulterações.

SPF e DKIM juntos: uma equipa para a sua segurança

SPF e DKIM são poderosos, mas dão o seu melhor quando trabalham em equipa. Utilizar ambos é como usar cinto e suspensórios: uma dupla garantia de segurança. O SPF assegura que o email provém de uma "estação de correios" autorizada, enquanto o DKIM garante que o "selo" no envelope é autêntico e não foi adulterado. Juntos, fornecem uma prova muito mais robusta da identidade do remetente. Para completar esta equipa de segurança, intervém um terceiro protocolo: o **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**.

O DMARC atua como um supervisor que, baseando-se nos resultados dos controlos SPF e DKIM, dá instruções precisas ao servidor de correio recetor sobre como tratar os emails que falham nos testes. O proprietário do domínio pode decidir se as mensagens não autenticadas devem ser colocadas em quarentena (na pasta de spam), rejeitadas totalmente, ou simplesmente monitorizadas. Este trio de protocolos é hoje o padrão de referência para a

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

segurança do correio eletrónico e representa uma arma formidável para as empresas que querem proteger a sua reputação e para os utilizadores que desejam uma caixa de correio mais limpa e segura. Muitos dos emails que não superam estes controlos são bloqueados automaticamente, como explicado no guia para filtrar o spam de forma eficaz.

Como reconhecer um email suspeito no Gmail e Outlook

Os principais fornecedores de correio eletrónico, como Gmail e Outlook, ajudam-nos a identificar as mensagens potencialmente perigosas através de sinais visuais claros. No **Gmail**, o sinal mais evidente é um **ponto de interrogação vermelho** ao lado do nome do remetente. Este símbolo indica que o Gmail não conseguiu verificar a identidade do remetente através de SPF ou DKIM. Se vir este aviso, especialmente num email que lhe pede dados pessoais ou para clicar em links, a prudência é obrigatória. Pode tratar-se de uma tentativa de phishing. É fundamental aprender a reconhecer e denunciar emails fraudulentos para proteger os seus dados.

Também o **Outlook** implementa sistemas de aviso semelhantes, mostrando frequentemente um banner na parte superior do email que alerta para a dificuldade de verificar a identidade do remetente. Além destes indicadores, outro sinal de alarme é a falta do logótipo da marca (tecnologia BIMI), que as empresas verificadas mostram frequentemente ao lado do seu nome. Prestar atenção a estes detalhes é um hábito simples mas poderoso. Se um email que parece provir do seu banco ou de um serviço online apresenta estes sinais, não clique em nenhum link. Contacte diretamente a empresa através dos seus canais oficiais para verificar a comunicação e considere blindar o seu Gmail

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

com a autenticação de dois fatores para um nível adicional de proteção.

O mercado italiano e o desafio da segurança do email

Em Itália, o tecido económico é composto em grande parte por pequenas e médias empresas (PME), que são frequentemente alvos privilegiados de ataques informáticos por serem consideradas menos estruturadas em termos de segurança. O Relatório Clusit 2024 destaca que o setor transformador e o governamental estão entre os mais afetados no país. Para estas realidades, um ataque de phishing bem-sucedido não significa apenas uma potencial perda económica, mas também um grave dano à reputação e à confiança dos clientes. Adotar protocolos como SPF, DKIM e DMARC já não é um luxo tecnológico, mas um investimento estratégico para a continuidade do negócio e a proteção da própria marca.

As próprias instituições, como a **Agenzia per l'Italia Digitale (AgID)**, promovem ativamente a adoção de padrões de segurança para a Administração Pública e para as empresas. O objetivo é criar um ecossistema digital nacional mais robusto e resiliente. Neste contexto, também o Correio Eletrónico Certificado (PEC), muito difundido em Itália, está a evoluir com sistemas de autenticação mais fortes para garantir o valor legal das comunicações. Para uma empresa, configurar corretamente estes protocolos é um passo fundamental que comunica profissionalismo e atenção à segurança, elementos cada vez mais apreciados num mercado competitivo. Esta atenção reflete-se também em detalhes como criar assinaturas de email profissionais, que contribuem para uma imagem empresarial coerente e fiável.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Conclusões

Navegar no mundo do correio eletrónico pode parecer complexo, mas compreender os mecanismos básicos que garantem a nossa segurança é mais simples do que se pensa. SPF, DKIM e DMARC já não são apenas siglas para especialistas em tecnologia, mas verdadeiros aliados na nossa vida digital quotidiana. Vimos como o SPF atua como controlador de passaportes, o DKIM como selo de garantia e o DMARC como supervisor inflexível. Juntos, formam uma barreira eficaz contra ameaças cada vez mais sofisticadas como o phishing e o spoofing.

A adoção destes protocolos, aliada a uma maior consciência dos sinais de perigo, como o ponto de interrogação vermelho no Gmail, permite-nos transformar a nossa caixa de correio de um potencial ponto fraco numa fortaleza segura. Num contexto como o italiano, onde a confiança e a reputação são valores centrais tanto nas relações pessoais como nas comerciais, proteger a própria identidade digital é um dever para consigo mesmo e para com os outros. Ser um utilizador informado é o primeiro e mais importante passo para uma experiência online serena e protegida.

Perguntas frequentes

O que significa o ponto de interrogação vermelho que vejo no Gmail ao lado do nome de quem me escreveu?

O ponto de interrogação vermelho no Gmail indica que a mensagem não superou os controlos de autenticação. Na prática, o Gmail não conseguiu verificar com certeza se o email provém realmente do remetente declarado, porque não foram configurados corretamente os protocolos de segurança como SPF (Sender Policy Framework) ou DKIM (DomainKeys Identified Mail). Embora

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

um email com este símbolo não seja automaticamente perigoso, é um aviso importante que o convida a prestar a máxima atenção: não clique em links, não descarregue anexos e não forneça dados pessoais.

O que são SPF e DKIM em palavras simples?

SPF e DKIM são dois sistemas que protegem a sua caixa de correio, um pouco como controlos de segurança para as cartas. O SPF (Sender Policy Framework) é como uma lista de carteiros autorizados: o proprietário de um domínio (ex. @empresa.pt) declara quais os servidores que podem enviar emails em seu nome. O DKIM (DomainKeys Identified Mail), por outro lado, é como um selo de cera num envelope: adiciona uma assinatura digital oculta ao email, que garante que o conteúdo não foi modificado durante a viagem. Juntos, estes dois protocolos ajudam os fornecedores como o Gmail a verificar se um email é autêntico e não uma tentativa de burla.

Como posso perceber se um email é uma tentativa de phishing?

Reconhecer um email de phishing requer atenção a vários detalhes. Antes de mais, verifique com cuidado o endereço do remetente, que muitas vezes imita o de empresas famosas mas com ligeiras diferenças. Desconfie das mensagens que usam uma linguagem alarmista ou criam um sentido de urgência, pressionando-o a agir rapidamente. Preste atenção a erros de gramática ou de ortografia e a saudações genéricas em vez do seu nome. Sobretudo, não clique em links suspeitos (pode passar o rato por cima sem clicar para ver o endereço real) e nunca descarregue anexos de remetentes desconhecidos ou duvidosos.

Tenho de configurar eu o SPF e DKIM para o meu email pessoal (ex. Gmail, Outlook)?

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Não, para uma conta de correio pessoal fornecida por grandes fornecedores como Gmail, Outlook ou Yahoo, não tem de fazer nada. São os próprios fornecedores que gerem a configuração de SPF, DKIM e outras medidas de segurança para garantir que os seus emails estão protegidos e autenticados. A configuração destes registos DNS é, pelo contrário, uma operação que diz respeito a quem possui um domínio personalizado (por exemplo, nome@omeudominio.pt) e o usa para enviar emails, como empresas, profissionais ou quem gere um site web.

SPF e DKIM sozinhos bastam para bloquear todos os emails falsos?

SPF e DKIM são fundamentais, mas não são suficientes por si só para uma proteção completa. Funcionam melhor quando combinados com o DMARC (Domain-based Message Authentication, Reporting, and Conformance). O DMARC é como uma instrução que o proprietário de um domínio dá aos servidores de correio recetores: diz-lhes o que fazer (rejeitar, colocar em spam ou aceitar) com os emails que não superam os controlos SPF ou DKIM. Juntos, estes três protocolos criam um sistema de defesa a vários níveis muito mais robusto contra phishing e spoofing.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati