SPF und DKIM: Der Leitfaden zum Erkennen gefälschter E-Mails

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

Jeden Tag herrscht in unserem E-Mail-Postfach ein reges Treiben, ein bisschen wie auf einem Dorfplatz während des Wochenmarktes. Es gibt geschäftliche Nachrichten, Newsletter, die wir abonniert haben, und persönliche Mitteilungen. Inmitten dieses Stroms verbergen sich jedoch auch täuschende Nachrichten, Betrugsversuche, die als Phishing bekannt sind. Wie können wir einen vertrauenswürdigen Absender von einem Betrüger unterscheiden? Die Antwort liegt in drei technisch anmutenden, aber intuitiv funktionierenden Kürzeln: **SPF, DKIM** und DMARC. Stellen wir sie uns als digitale Ausweisdokumente vor, die es ermöglichen, die Echtheit des Absenders zu überprüfen, und so die Tradition des Vertrauens mit einer für unsere Sicherheit unverzichtbaren technologischen Innovation verbinden.

Diese Protokolle sind keine abstrakten Konzepte nur für Fachleute. Im Gegenteil, sie stellen die erste Verteidigungslinie gegen Cyberbetrug dar. Ihre Funktionsweise zu verstehen bedeutet, sich mit den Werkzeugen auszustatten, um bewusster durch die digitale Welt zu navigieren. Dieser Artikel entstand mit dem Ziel, diese Fachbegriffe in eine einfache und direkte Sprache zu übersetzen, um jedem, unabhängig von seinen Computerkenntnissen, zu helfen, sein digitales Leben zu schützen. Wir werden gemeinsam lernen, die Signale einer verdächtigen E-Mail zu erkennen und unser Postfach in einen sichereren Ort zu verwandeln.

Warum Vertrauen in E-Mails wie ein Händedruck ist

In der mediterranen Kultur hat ein Händedruck schon immer eine Vereinbarung besiegelt und einen Vertrauenspakt dargestellt. In der digitalen Welt ist dieses Vertrauen ebenso grundlegend, aber viel zerbrechlicher. Die häufigste Gefahr ist das *Spoofing*, eine Technik, mit der ein Angreifer die Absenderadresse fälscht, um den Anschein zu erwecken, die E-Mail stamme von einer vertrauenswürdigen Quelle, wie unserer Bank, einem Kurierdienst oder sogar einem Kollegen. Das Ziel ist fast immer, uns zu schädlichen Handlungen zu verleiten, wie der Preisgabe von Passwörtern oder Finanzdaten. Diese Bedrohung ist alles andere als selten; vielmehr ist sie eine der Hauptursachen für Cybervorfälle.

Die Daten bestätigen den Ernst des Problems. Laut dem Clusit-Bericht 2024 sind Cyberangriffe in Italien im Vergleich zum Vorjahr um 65 % gestiegen, und Phishing ist eine der am weitesten verbreiteten Techniken. Diese alarmierende Statistik verdeutlicht, dass die Fähigkeit, die Identität des Absenders zu überprüfen, keine Option mehr ist, sondern eine Notwendigkeit. Genauso wie Sie einem Fremden nicht die Haustür öffnen würden, ist es entscheidend zu lernen, E-Mails von nicht verifizierten Absendern nicht zu “öffnen”. Authentifizierungsprotokolle wie SPF und DKIM sind die Werkzeuge, die uns genau das ermöglichen: zu kontrollieren, wer an unsere digitale Tür klopft.

SPF: Der Kontrolleur der digitalen Pässe

Das Protokoll **SPF (Sender Policy Framework)** kann man sich als einen strengen Passkontrolleur an der digitalen Grenze vorstellen. Einfach ausgedrückt veröffentlicht der Inhaber einer Domain (z. B. `meinebank.de`) eine offizielle Liste autorisierter “Postboten”, also der Mailserver, die die

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Erlaubnis haben, E-Mails in seinem Namen zu versenden. Diese Liste ist öffentlich und im Domain Name System (DNS) registriert, einer Art Telefonbuch des Internets. Wenn wir eine E-Mail erhalten, überprüft unser E-Mail-Provider (wie Gmail oder Outlook) die IP-Adresse des Servers, der sie gesendet hat, und vergleicht sie mit der vom Absender-Domain autorisierten Liste.

Wenn die IP-Adresse des sendenden Servers in der SPF-Liste enthalten ist, wird der “Pass” abgestempelt und die E-Mail als legitim betrachtet. Andernfalls kennzeichnet der Mailserver sie als verdächtig, meldet sie oder blockiert sie in einigen Fällen sogar, bevor sie unseren Posteingang erreicht. Dieser Mechanismus ist eine erste, grundlegende Barriere gegen Spoofing. Er hindert einen Betrüger daran, einen nicht autorisierten Server zu verwenden, um E-Mails im Namen unserer Bank zu versenden, da sein “digitaler Pass” sofort als ungültig erkannt würde. Es ist ein System, das auf Transparenz und Überprüfung basiert, ein Pfeiler für den Aufbau einer sichereren E-Mail-Umgebung.

DKIM: Das Wachssiegel im digitalen Zeitalter

Während SPF kontrolliert, wer eine Nachricht versenden darf, fungiert **DKIM (DomainKeys Identified Mail)** wie ein Wachssiegel auf einem antiken Brief und garantiert dessen Echtheit und Integrität. Dieses Protokoll fügt dem Header jeder gesendeten E-Mail eine eindeutige digitale Signatur hinzu. Die Signatur wird mit einem privaten Schlüssel erstellt, der geheim und nur dem Server des Absenders bekannt ist. Der entsprechende öffentliche Schlüssel ist hingegen für alle über die DNS-Einträge der Domain zugänglich, genau wie die SPF-Liste. Wenn die E-Mail am Zielort ankommt, verwendet der Server des Empfängers den öffentlichen Schlüssel, um die digitale Signatur zu überprüfen.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Wenn die Überprüfung erfolgreich ist, bedeutet das zwei wesentliche Dinge. Erstens: Die E-Mail stammt tatsächlich von der angegebenen Domain, da nur der rechtmäßige Eigentümer den privaten Schlüssel besitzt, um diese spezifische Signatur zu erstellen. Zweitens: Der Inhalt der Nachricht wurde während der Übertragung nicht verändert. Jede Änderung, auch die kleinste, würde die Signatur ungültig machen, genau wie ein gebrochenes Wachssiegel verraten würde, dass der Brief geöffnet wurde. DKIM authentifiziert also nicht nur den Absender, sondern schützt auch die Integrität der Nachricht und stellt sicher, dass das, was wir lesen, genau das ist, was geschrieben wurde, ohne Manipulationen.

SPF und DKIM gemeinsam: Ein Team für Ihre Sicherheit

SPF und DKIM sind leistungsstark, aber sie funktionieren am besten, wenn sie im Team arbeiten. Beide zu verwenden ist wie das Tragen von Gürtel und Hosenträgern: eine doppelte Sicherheitsgarantie. SPF stellt sicher, dass die E-Mail von einem autorisierten “Postamt” stammt, während DKIM garantiert, dass das “Siegel” auf dem Umschlag echt ist und nicht manipuliert wurde. Zusammen liefern sie einen viel robusteren Beweis für die Identität des Absenders. Um dieses Sicherheitsteam zu vervollständigen, greift ein drittes Protokoll ein: **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**.

DMARC agiert als Aufseher, der basierend auf den Ergebnissen der SPF- und DKIM-Prüfungen dem empfangenden Mailserver genaue Anweisungen gibt, wie mit E-Mails zu verfahren ist, die die Tests nicht bestehen. Der Domaininhaber kann entscheiden, ob nicht authentifizierte Nachrichten unter Quarantäne

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

gestellt (in den Spam-Ordner verschoben), vollständig abgelehnt oder einfach überwacht werden sollen. Dieses Trio von Protokollen ist heute der Goldstandard für E-Mail-Sicherheit und stellt eine formidable Waffe für Unternehmen dar, die ihren Ruf schützen wollen, sowie für Benutzer, die ein saubereres und sichereres Postfach wünschen. Viele E-Mails, die diese Kontrollen nicht bestehen, werden automatisch blockiert, wie im Leitfaden zum effektiven Filtern von Spam erklärt.

Wie man eine verdächtige E-Mail in Gmail und Outlook erkennt

Die wichtigsten E-Mail-Anbieter wie Gmail und Outlook helfen uns durch klare visuelle Signale, potenziell gefährliche Nachrichten zu identifizieren. Bei **Gmail** ist das auffälligste Signal ein **rotes Fragezeichen** neben dem Namen des Absenders. Dieses Symbol zeigt an, dass Gmail die Identität des Absenders nicht über SPF oder DKIM verifizieren konnte. Wenn Sie diesen Warnhinweis sehen, insbesondere in einer E-Mail, die nach persönlichen Daten fragt oder Sie zum Klicken auf Links auffordert, ist Vorsicht geboten. Es könnte sich um einen Phishing-Versuch handeln. Es ist wichtig zu lernen, Betrugs-E-Mails zu erkennen und zu melden, um die eigenen Daten zu schützen.

Auch **Outlook** implementiert ähnliche Warnsysteme und zeigt oft ein Banner im oberen Teil der E-Mail an, das vor der Schwierigkeit warnt, die Identität des Absenders zu überprüfen. Neben diesen Indikatoren ist ein weiteres Warnsignal das Fehlen des Markenlogos (BIMI-Technologie), das verifizierte Unternehmen oft neben ihrem Namen anzeigen. Auf diese Details zu achten, ist eine einfache, aber wirkungsvolle Gewohnheit. Wenn eine E-Mail, die scheinbar von Ihrer Bank oder einem Online-Dienst stammt, diese Signale aufweist, klicken

Sie auf keinen Link. Kontaktieren Sie das Unternehmen direkt über seine offiziellen Kanäle, um die Kommunikation zu überprüfen, und ziehen Sie in Erwägung, Ihr Gmail mit der Zwei-Faktor-Authentifizierung abzusichern, um eine zusätzliche Schutzebene zu erhalten.

Der italienische Markt und die Herausforderung der E-Mail-Sicherheit

In Italien besteht das wirtschaftliche Gefüge größtenteils aus kleinen und mittleren Unternehmen (KMU), die oft bevorzugte Ziele von Cyberangriffen sind, da sie in Bezug auf Sicherheit als weniger strukturiert gelten. Der Clusit-Bericht 2024 hebt hervor, dass der verarbeitende Sektor und der Regierungssektor zu den am stärksten betroffenen Bereichen in unserem Land gehören. Für diese Realitäten bedeutet ein erfolgreicher Phishing-Angriff nicht nur einen potenziellen wirtschaftlichen Verlust, sondern auch einen schweren Schaden für den Ruf und das Vertrauen der Kunden. Die Einführung von Protokollen wie SPF, DKIM und DMARC ist kein technologischer Luxus mehr, sondern eine strategische Investition für die Geschäftskontinuität und den Schutz der eigenen Marke.

Die Institutionen selbst, wie die **Agentur für das digitale Italien (AgID)**, fördern aktiv die Einführung von Sicherheitsstandards für die öffentliche Verwaltung und für Unternehmen. Ziel ist es, ein robusteres und widerstandsfähigeres nationales digitales Ökosystem zu schaffen. In diesem Zusammenhang entwickelt sich auch die in Italien weit verbreitete zertifizierte E-Mail (PEC) mit stärkeren Authentifizierungssystemen weiter, um den rechtlichen Wert der Kommunikation zu gewährleisten. Für ein Unternehmen ist die korrekte Konfiguration dieser Protokolle ein grundlegender Schritt, der

Professionalität und Aufmerksamkeit für Sicherheit vermittelt – Elemente, die in einem wettbewerbsintensiven Markt immer mehr geschätzt werden. Diese Aufmerksamkeit spiegelt sich auch in Details wider, wie dem Erstellen professioneller E-Mail-Signaturen, die zu einem konsistenten und zuverlässigen Unternehmensimage beitragen.

Fazit

Sich in der Welt der E-Mails zurechtzufinden mag komplex erscheinen, aber die grundlegenden Mechanismen zu verstehen, die unsere Sicherheit gewährleisten, ist einfacher als man denkt. SPF, DKIM und DMARC sind nicht mehr nur Kürzel für Technologieexperten, sondern echte Verbündete in unserem digitalen Alltag. Wir haben gesehen, wie SPF als Passkontrolleur, DKIM als Garantiesiegel und DMARC als unnachgiebiger Aufseher fungiert. Zusammen bilden sie eine wirksame Barriere gegen immer ausgefeiltere Bedrohungen wie Phishing und Spoofing.

Die Einführung dieser Protokolle, kombiniert mit einem größeren Bewusstsein für Gefahrensignale wie das rote Fragezeichen in Gmail, ermöglicht es uns, unser Postfach von einem potenziellen Schwachpunkt in eine sichere Festung zu verwandeln. In einem Kontext wie dem italienischen, in dem Vertrauen und Reputation sowohl in persönlichen als auch in geschäftlichen Beziehungen zentrale Werte sind, ist der Schutz der eigenen digitalen Identität eine Pflicht gegenüber sich selbst und anderen. Ein informierter Benutzer zu sein, ist der erste und wichtigste Schritt für eine sorgenfreie und geschützte Online-Erfahrung.

Häufig gestellte Fragen

Was bedeutet das rote Fragezeichen, das ich in Gmail neben dem Namen des Absenders sehe?

Das rote Fragezeichen in Gmail zeigt an, dass die Nachricht die Authentifizierungsprüfungen nicht bestanden hat. Praktisch bedeutet dies, dass Gmail nicht mit Sicherheit verifizieren konnte, dass die E-Mail wirklich vom angegebenen Absender stammt, da Sicherheitsprotokolle wie SPF (Sender Policy Framework) oder DKIM (DomainKeys Identified Mail) nicht korrekt konfiguriert wurden. Obwohl eine E-Mail mit diesem Symbol nicht automatisch gefährlich ist, ist es ein wichtiger Warnhinweis, der Sie zu höchster Aufmerksamkeit auffordert: Klicken Sie nicht auf Links, laden Sie keine Anhänge herunter und geben Sie keine persönlichen Daten preis.

Was sind SPF und DKIM in einfachen Worten?

SPF und DKIM sind zwei Systeme, die Ihr E-Mail-Postfach schützen, ähnlich wie Sicherheitskontrollen für Briefe. SPF (Sender Policy Framework) ist wie eine Liste autorisierter Postboten: Der Inhaber einer Domain (z. B. @firma.de) erklärt, welche Server E-Mails in seinem Namen versenden dürfen. DKIM (DomainKeys Identified Mail) hingegen ist wie ein Wachssiegel auf einem Umschlag: Es fügt der E-Mail eine versteckte digitale Signatur hinzu, die garantiert, dass der Inhalt während der Reise nicht verändert wurde. Zusammen helfen diese beiden Protokolle Anbietern wie Gmail zu überprüfen, ob eine E-Mail authentisch ist und kein Betrugsversuch.

Woran erkenne ich, ob eine E-Mail ein Phishing-Versuch ist?

Das Erkennen einer Phishing-E-Mail erfordert Aufmerksamkeit für verschiedene Details. Überprüfen Sie zunächst sorgfältig die Absenderadresse, die oft die von bekannten Unternehmen nachahmt, aber leichte Unterschiede aufweist.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

Misstrauen Sie Nachrichten, die eine alarmierende Sprache verwenden oder ein Gefühl der Dringlichkeit erzeugen, um Sie zu schnellem Handeln zu drängen. Achten Sie auf Grammatik- oder Rechtschreibfehler und auf allgemeine Anreden anstelle Ihres Namens. Klicken Sie vor allem nicht auf verdächtige Links (Sie können mit der Maus darüberfahren, ohne zu klicken, um die tatsächliche Adresse zu sehen) und laden Sie niemals Anhänge von unbekannten oder zweifelhaften Absendern herunter.

Muss ich SPF und DKIM für meine persönliche E-Mail (z. B. Gmail, Outlook) konfigurieren?

Nein, für ein persönliches E-Mail-Konto, das von großen Anbietern wie Gmail, Outlook oder Yahoo bereitgestellt wird, müssen Sie nichts tun. Die Anbieter selbst verwalten die Konfiguration von SPF, DKIM und anderen Sicherheitsmaßnahmen, um sicherzustellen, dass Ihre E-Mails geschützt und authentifiziert sind. Die Konfiguration dieser DNS-Einträge ist hingegen eine Aufgabe für diejenigen, die eine eigene Domain besitzen (z. B. name@meinedomain.de) und diese zum Versenden von E-Mails nutzen, wie Unternehmen, Freiberufler oder Website-Betreiber.

Reichen SPF und DKIM allein aus, um alle gefälschten E-Mails zu blockieren?

SPF und DKIM sind grundlegend, reichen aber allein für einen vollständigen Schutz nicht aus. Sie funktionieren am besten, wenn sie mit DMARC (Domain-based Message Authentication, Reporting, and Conformance) kombiniert werden. DMARC ist wie eine Anweisung, die der Domaininhaber den empfangenden Mailservern gibt: Es sagt ihnen, was sie mit E-Mails tun sollen (abweisen, in den Spam verschieben oder akzeptieren), die die SPF- oder DKIM-Prüfungen nicht bestehen. Zusammen schaffen diese drei Protokolle ein viel

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati

robusteres, mehrschichtiges Verteidigungssystem gegen Phishing und Spoofing.

Copyright © 2026 TuttoSemplice.com - Tutti i diritti riservati