1/ Thiếu bản ghi SPF - Xác thực quyền gửi email cho hệ thống Google.

=> Cần bổ sung bản ghi này để email gửi đi tránh bị rơi vào mục spam, hướng dẫn [tại đây](https://support.google.com/a/answer/33786?hl=en).

2/ Thiếu bản ghi DKIM - Chữ ký điện tử bảo mật emai

=> Bổ sung bản ghi này giúp tăng tính bảo mật và độ uy tín của thư gửi đi, hướng dẫn chi tiết [tại đây](https://support.google.com/a/answer/174124?hl=en).

3/ Thiếu bản ghi DMARC - chính sách bảo vệ hệ thống email khỏi email phishing và spoofing

=> Đây là bản ghi đặc biệt quan trọng nhằm bảo vệ hệ thống email, đề phòng rủi ro lừa đảo và giả mạo qua email, hướng dẫn chi tiết [tại đây](https://support.google.com/a/answer/2466580?hl=en&ref_topic=2759254).

1. Có force quy định đặt mật khẩu khó và đổi password định kỳ không?

2. Có support nhắc đổi password định kỳ  tự động không. (trường hợp không dùng script của a.Giang)

3. Có làm được các access list như:

- Nhóm chỉ nhận mail trong Cty

- Nhóm chỉ nhận mail từ 1 số domain xác định

- Chỉ cho phép check mail từ 1 vài địa chỉ ip

...

4. Gói này có support generate các báo cáo không ? :) cái này chắc hơi khó.

- Tạo báo cáo theo mẫu nào đấy : vd : tổng số account đang active/số account 90 ngày không  hoạt động.,,,

DMARC là gì? Tầm quan trọng của nó với Mail Server như thế nào?

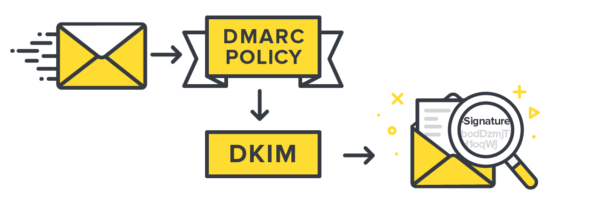
**DMARC là gì?**

DMARC là một tiêu chuẩn để chặn spammer khỏi việc sử dụng domain của người sở hữu mà không được sự cho phép của họ mà ta hay gọi nó là spoofing. Thực tế, khi sử dụng mail, bất kỳ ai cũng có thể giả mạo địa chỉ tại trường “From” trong mail gửi đi một cách dễ dàng. DMARC sẽ đảm bảo những mail giả mạo này sẽ bị chặn trước khi chúng đến được mailbox của người nhận và hơn thế nữa, chỉ những mail hợp lệ mới được chấp nhận vào hệ thống.

**DMARC hoạt động như thế nào?**

DMARC được xây dựng ở phía trên của DKIM và SPF. Vậy trước tiên, ta sẽ xem DKIM và SPF là gì?

**DKIM (Domainkeys Identified Mail)**

[](https://1hosting.com.vn/wp-content/uploads/2016/05/dmarc-dkim.png)

DKIM là một phương thức để xác thực tính hợp lệ của một email. Mỗi mail khi gửi đi được gắn 1 khóa private key và sau đó được xác thực bên phía mail server nhận bằng một khóa public key được setup trong bản ghi DNS. Quá trình này đảm bảo rằng mail gửi đi không bị thay đổi trên đường tới phía bên nhận. Nói cách khác, nó ngăn chặn ai đó có thể can thiệp vào email của bạn, thay đổi nó và sau đó gửi đi với nội dung mới. Bản chất của nó giống hệt như giao thức SSH mà ta vẫn hay dùng hàng ngày.

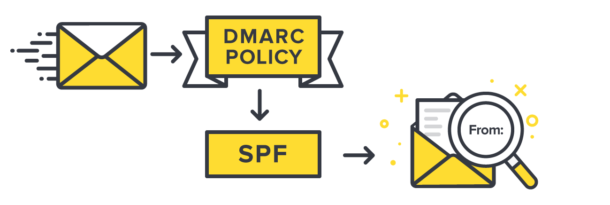
DKIM còn giúp các ISP sử dụng những thông tin đó để đánh giá mực độ tin cậy của domain bằng một thông số ta vẫn thường nghe là “*reputation*“. Việc thực hiện gửi mail một cách lành mạnh với tỉ lệ SPAM và bounces ít, tỉ lệ chấp nhận cao sẽ tự nhiên làm tăng độ tin cậy và xác thực của domain đó đối với các ISP

Đây là cách setup DKIM trong DNS mà ta vẫn thường thấy với public key:

pm.\_domainkey.domain.com IN TXT

k=rsa\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOCTHqIIQhGNISLchxDvv2X8NfkW7MEHGmtawoUgVUb8V1vXhGikCwYNqFR5swP6UCxCutX81B3+5SCDJ3rMYcu3tC/E9hd1phV+cjftSFLeJ+xe+3xwK+V18kM46kBPYvcZ/38USzMBa0XqDYw7LuMGmYf3gA/yJhaexYXa/PYwIDAQAB

**SPF (Sender Policy Framework)**

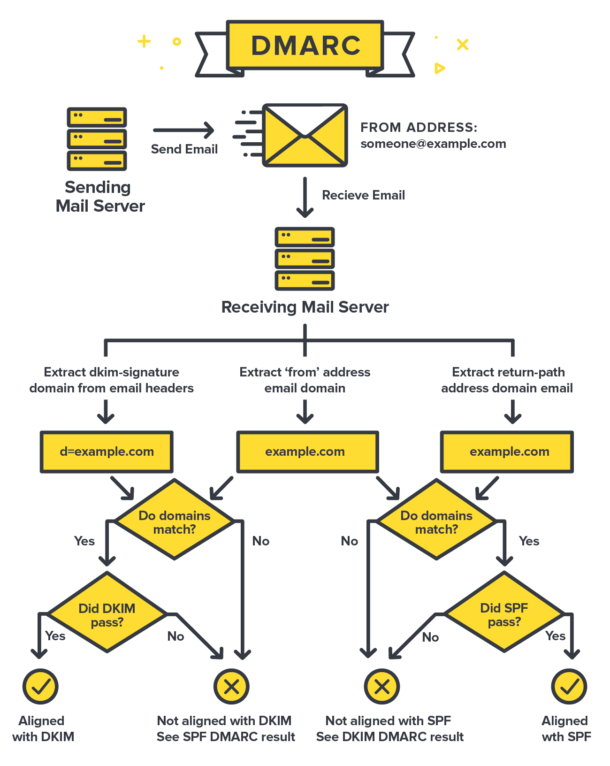
[](https://1hosting.com.vn/wp-content/uploads/2016/05/dmarc-spf.png)

SPF là một cách thức để xác nhận một email server có được phép gửi email dưới tên một domain nào đó không. Chẳng hạn như muốn email từ domain @1hosting.com.vn chỉ có giá trị khi gửi từ địa chỉ IP *123.345.456.789*, còn các mail server có IP khác mà gửi các mail có đuôi @1hosting.com.vn đều là giả mạo và không được phép thì SPF sẽ thực hiện điều này. Khi đó mail server phía nhận sẽ tự động loại bỏ tất cả các email gửi dưới dạng @1hosting.com.vn từ các địa chỉ không phải IP *123.345.456.789.*Tất nhiên mail server phía nhận phải có chức năng kiểm tra SPF này, còn không kiểm tra thì có cấu hình cũng bằng thừa*.*

**DMARC kết hợp DKIM và SPF**

DMARC tiến một bước xa hơn so với DKIM và SPF khi nó cho ta quyền thiết lập một policy để loại bỏ (reject) hay cách ly (quarantine- thường hành động là cho mail này vào SPAM folder) một email từ một nguồn không rõ ràng hoặc không có độ tin cậy dựa trên kết quả của DKIM và SPF.

DMARC cho phép ta nói với các Mail server phía bên nhận cách thức xử lý khi SPF hay DKIM failed hoặc không có. Dưới đây là môt mô tả cách thức SPF và DKIM cùng làm việc với DMARC.

[](https://1hosting.com.vn/wp-content/uploads/2016/05/DMARC.png)

DMARC policy được setup trong DNS và trông giống như sau:

\_dmarc.domain.com TXT v=DMARC1\; p=reject\; pct=100\; rua=mailto:dmarc-reports@domain.com\;

Bản ghi trên tạo 1 policy để reject (p=reject) 100% (pct=100) các email không pass DKIM hay SPF. Bên cạnh đó, bản ghi còn cho biết lý do từ chối sẽ được gửi vào mail (rua=mailto:dmarc-reports@domain.com) để người quản trị phía domain.com được biết.

**Triển khai DMARC trên domain như thế nào?**

Cấu hình DMARC cho một domain là phần vô cùng nhậy cảm và sẽ mất nhiều thời gian vì sẽ có rủi ro trong quá trình thực hiện. Rủi ro đó là khi cấu hình DMARC sẽ có thể loại bỏ cả những mail hợp lệ. Để tránh điều này, ta cần thực hiện theo trình tự quan sát rồi áp dụng sau (áp dụng ngay sẽ khiến gặp rất nhiều vấn đề)

***Bước 1: Tạo một bản ghi DMARC để bắt đầu theo dõi***

Chẳng hạn ta tạo 1 bản ghi như sau:

\_dmarc.domain.com TXT v=DMARC1\; p=none\; pct=100\; rua=mailto:dmarc-reports@domain.com\;

Bản ghi này giống như ví dụ trên nhưng khác ở chỗ “p=none” thay vì “p=reject”. “none” cho biết đây là chế độ test mode. Các mail server nhận sẽ check từng message gửi đến nhưng nó chi gửi về các report mà không thực hiện hành động nào cụ thể. Điều này cho phép ta thu thập được thông tin chi tiết về các địa chỉ mail server gửi đến trước khi có quyết định thực hiện một hành động cụ thể.

Lúc này ta cần một công cụ để thu thập những số liệu thống kê này và [http://dmarc.postmarkapp.com](http://dmarc.postmarkapp.com/) là công cụ không thể bỏ qua

***Bước 2: Phân tích DMARC report để xác định kết quả pass hay fail***

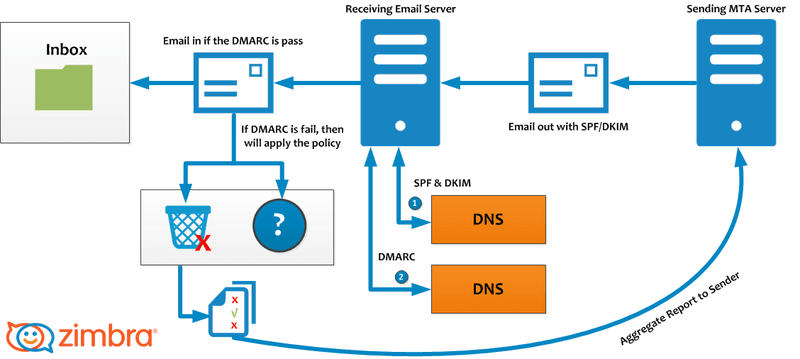
DKIM giống với SPF có vai trò cực kỳ quan trọng trong việc xác nhận giả mạo và những spam mail đang có xu hướng gia tăng ngày một nhiều hiện nay có thể nói DKIM đóng vai trò như là tấm chắn giúp bạn giảm bớt độc tố đến cơ thể vậy chi tiết về **DKIM là gì ? Hướng dẫn cấu hình DKIM để xác nhận email hợp lệ** tất cả sẽ có trong bài viết này của Tinomail.

## **DKIM là gì ? https://tinomail.com/wp-content/uploads/2018/06/IC850812.jpg**

DKIM là viết tắt của từ **Domain Keys Identified Mail**đây là một phương thức giúp xác nhận các email giúp tránh email giả, nó được thiết kế để cho phép người nhận kiểm tra email được xác nhận là đến từ tên miền cụ thể nào? và thực tự tên miền này có được ủy quyền hay không ? DKIM được thiết kế để ngăn chặn các địa chỉ người gửi giả mạo trong email một trong những kỹ thuật thường được sử dụng nhất hiện nay đó là thư lừa đảo và email spam gửi các mã độc tấn công.

## **Tìm hiểu tổng quan về DKIM**

DKIM cung cấp cho hai hoạt động riêng biệt, là chữ ký và xác minh. Một trong số chúng có thể được xử lý bởi một mô-đun của một tác nhân chuyển thư (MTA). Tổ chức ký kết sử dụng có thể là người xử lý trực tiếp thư, chẳng hạn như tác giả, trang gửi hoặc trung gian tiếp theo dọc theo đường chuyển tuyến của thư hoặc người xử lý gián tiếp như dịch vụ độc lập cung cấp hỗ trợ cho người xử lý trực tiếp. Các mô-đun ký hiệu chèn một hoặc nhiều DKIM-Signature:trường tiêu đề, có thể thay mặt cho tổ chức tác giả hoặc nhà cung cấp dịch vụ gốc. Việc xác minh các mô-đun thường hành động thay mặt cho tổ chức người nhận , có thể ở mỗi bước gửi.



DKIM ra đời là kết quả của sự kết hợp giữa, “enhanced DomainKeys” của Yahoo và “Identified Internet Mail” của Cisco . Việc sáp nhập này là cơ sở cho một loạt các thông số kỹ thuật theo tiêu chuẩn IETF và các tài liệu hỗ trợ mà cuối cùng dẫn đến STD 76 , hiện tại đang sử dụng là RFC 6376 .  “Identified Internet Mail” được Cisco đề xuất như một tiêu chuẩn xác thực thư dựa trên chữ ký, trong khi DomainKey được thiết kế bởi Yahoo để xác minh  tên miền [DNS](https://tinomail.com/dns-la-gi) của người gửi e-mail và tính toàn vẹn của thư .

Các khía cạnh của DomainKeys, cùng với các phần của Identified Internet Mail, được kết hợp để tạo Thư được xác định tên miền (DKIM). Nhà cung cấp dịch vụ xu hướng triển khai DKIM bao gồm Yahoo , Gmail , AOL và FastMail . Bất kỳ thư nào từ các tổ chức này đều phải mang theo chữ ký DKIM.