Cơ chế bảo mật HSTS là gì? HSTS hoạt động như thế nào?

[12/10/2017](https://ssl.vn/co-che-bao-mat-hsts-la-gi-hsts-hoat-dong-nhu-the-nao.html) [Hoàng Tùng](https://ssl.vn/author/tunghv)



HSTS (HTTP Strict Transport Security) là một giao thức bảo mật mới yêu cầu tất cả kết nối tới một website phải được mã hóa bằng giao thức HTTPS. Hiện nay Google đang áp dụng HSTS cho 45 tên miền cao cấp nhất, bao gồm các tên miền có đuôi .google, .how và .soy. Vậy HSTS hoạt động như thế nào?



**Cái chết của giao thức HTTP**

HTTP là giao thức thời kì đầu của các website, vì vậy mà hiện nay HTTP luôn đứng trước nguy cơ tấn công. Hacker dễ dàng xâm nhập vào các đường truyền để thực hiện các cuộc tấn công hạ cấp hoặc tận dụng các kỹ thuật khác để cướp cookies ăn trộm thông tin. [**HTTPS**](https://ssl.vn/http-la-gi-tai-sao-nen-su-dung-https.html) đang được nhiều người sử dụng hơn bởi đảm bảo thông tin truyền đi khi người dùng truy cập vào website đã được mã hoá.

Theo thống kê bởi Wired thì có đến hơn nửa các website trên thế giới sử dụng giao thức HTTPS. Vào những năm 2010, Google cũng đã thử nghiệm những giao thức bảo mật mới trên Gmail nhằm tìm ra phương thức bảo mật mới. Nhưng đến năm 2014, Google đã công nhận và đặt hết niềm tin vào HTTPS. Năm ngoái, Google còn trở thành nhà tài trợ bạch kim của dịch vụ Let’s Encrypt nhằm cung cấp chứng chỉ SSL miễn phí cho các website.

Google cũng tăng nhận thức lên người dùng khi trình duyệt Chrome hiển thị thông báo cho người dùng những web sử dụng HTTP là không an toàn bảo mật. Theo đó, nhiều doanh nghiệp lớn đã chuyển sang HTTPS.

HTTPS là lựa chọn tối ưu dành cho website trong thời điểm ăn cắp thông tin người dùng đang ngày càng cao. Giờ đây, Google đang tiến hành các bước tiếp theo nhằm bảo đảm các kết nối đều an toàn bằng cách thực hiện chính sách bảo mật HSTS.

Cơ chế tải trước

HSTS là một hệ thống dựa trên thời gian, nghĩa là trong khoảng thời gian bạn thiết lập trong max-age (tính bằng giây) sẽ đảm bảo rằng trang web của bạn được phục vụ qua giao thức HTTPS.

Khi trình duyệt tương tác với máy chủ web đã bật HSTS, cơ chế tải trước sẽ tìm một header đặc biệt nói rằng trình duyệt chỉ nên sử dụng giao thức HTTPS để kết nối với server.

Ngay cả khi người dùng nhập vào một địa chỉ HTTP thì HSTS cũng sẽ tự động chuyển trang sang HTTPS trước khi tải. Thiết lập này được hỗ trợ trên Chrome, Firefox, Safari, Internet Explorer, Edge và Opera. Ben McIlwain, kỹ sư phần mềm của Google Registry, cho rằng rằng “việc sử dụng HSTS sẽ giúp đảm bảo an toàn mặc định cho mọi kết nối”.

Ngoài .google, Google còn thực hiện HSTS cho các tên miền có đuôi .how và .soy nhằm bán cho các công ty hoặc cá nhân muốn thiết lập trang web của riêng họ. Các đuôi khác như .ads, .boo, .here và .meme vẫn chưa được phát hành. Tuy nhiên, vì Google vốn quan tâm đặc biệt về bảo mật ở mức cao nhất, thế nên mọi kế hoạch áp dụng HSTS cho các tên miền cao cấp khác cũng sẽ được thúc đẩy sớm thôi.

Quyết định ở người dùng

HSTS tuy tăng tính bảo mật lên tối đa nhưng vẫn gặp những tranh cãi: Người dùng không thể truy cập vào các trang web HTTP mặc dù họ có nhu cầu và chấp nhận rủi ro? Vậy trải nghiệm duyệt web là của người dùng hay của HSTS?

Khi HTTP đã trở nên lỗi thời thì việc Google áp dụng HSTS để chuyển mọi trang web trở về HTTPS là hợp lý. Giống như khi Microsoft “khai tử” các phiên bản cũ và lỗi thời của Windows, Google cũng làm như vậy với HTTP.

Cơ chế tải trước của HSTS chỉ đơn giản hỗ trợ người dùng bảo mật web, còn việc sử dụng vẫn thuộc về phía người dùng.