Phân biệt HTTPS, SLL, thanh Address

Đã bao giờ bạn tự hỏi tại sao trên thanh địa chỉ website của bạn đường dẫn hiển thị lúc thì màu xanh lá cây lúc thì các biểu tượng khác nhau?. Một số trang Web, chữ màu xanh lá cây với tên của công ty sỡ hữu. Và nếu bạn để ý bạn sẽ thấy có sự phân biệt rõ ràng giữa chúng.

Nhìn vào hình trên với các Tab trên thanh địa chỉ website khác nhau, bốn điểm truy cập khác nhau, cái thì màu xanh lá cây, cái thì đơn sắc không có gì. Vậy ý nghĩa của nó là gì? Tất nhiên người ta không vô cớ làm như vậy, tất cả đều có lý do. Một sự phân biệt rõ ràng giữa nội dung an toàn và không an toàn. Chúng ta cần phải nắm rõ một số khái niệm để giải đáp thắc mắc về các biểu tượng với màu sắc khác nhau đó.

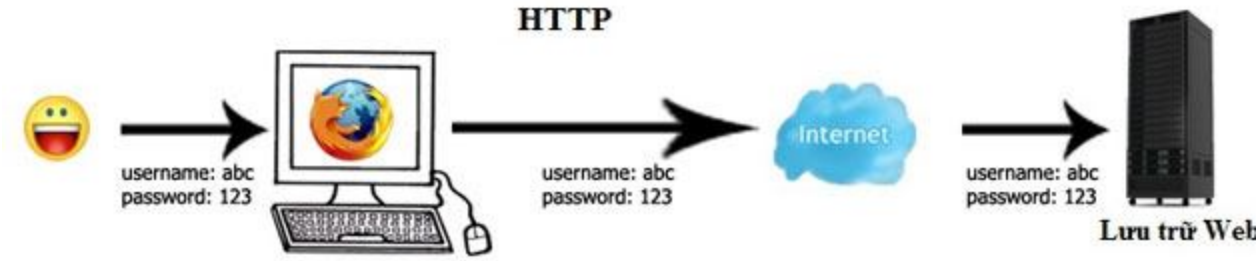
Vậy thế nào là nội dung an toàn và không an toàn?

Để hiểu đâu là nội dung an toàn đâu là nội dung không an toàn ta xem xét HTTPS và SSL, đó là 2 giao thức bảo mật quan trọng.

HTTP là viết tắt của Hypertext Transfer Protocol (Giao thức truyền tải siêu văn bản), đây là một cách thức truyền tải dữ liệu trên mạng Internet. Chúng ta thường gặp giao thức

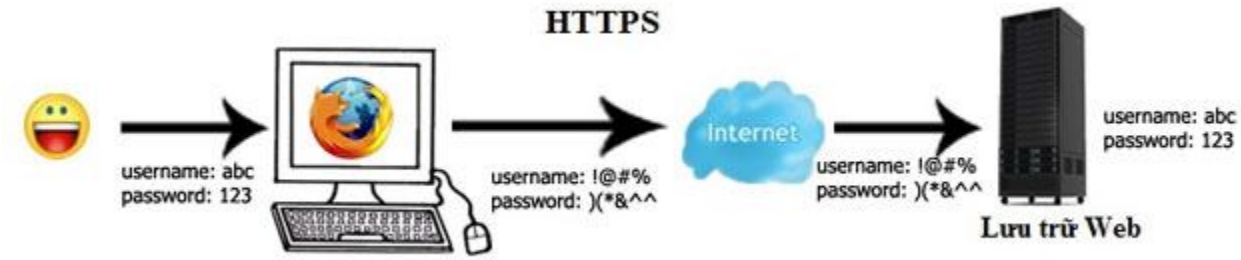
HTTP này khi sử dụng các trình duyệt web (như Firefox, chrome, IE…), khi chúng ta load website thông thường, chúng ta dùng giao thức HTTP để gửi và nhận dữ liệu.

Ngoài việc thấy ở trình duyệt, một số ứng dụng hiện tại cũng đang sử dụng cơ chế HTTP để truyền tải dữ liệu, ví dụ điển hình nhất là Yahoo.



HTTPS là viết tắt của Hypertext Transfer Protocol Secure (Giao thức truyền tải siêu văn bản có bảo mật). Chúng ta có thể đoán được là HTTPS khác HTTP ở điểm nào. Đó chính là HTTPS hỗ trợ thêm bảo mật, nó giải quyết vấn đề thông tin gửi nhận lên Internet của chúng ta bị rò rỉ.

HTTPS thường được sử dụng trong những trường hợp đăng nhập, đăng ký, thanh toán tiền, thanh toán thẻ,… Chúng là những thông tin nhạy cảm cần được bảo vệ.



SSL là từ viết tắt của Secure Socket Layer, là công nghệ nền tảng sử dụng giao thức HTTPS đảm bảo nội dung HTTP được mã hóa an toàn. Đơn giản, HTTPS là HTTP qua SSL. Nó là một sự kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS cho phép trao đổi thông tin một cách bảo mật trên Internet. HTTP không được mã hóa thông qua HTML giữa phía client và server.

Đó là lý do vì sao các trang Web như Ngân hàng, giao dịch thương mại,… chọn giao thức HTTPS. Vì HTTPS là sự lựa chọn cần thiết để bảo vệ an toàn cho các tài khoản nhạy cảm. Tuy nhiên, tốc độ tải trang sẽ bị chậm lại, không nhanh như HTTP. Vì thế nên các trang Web điện tử thường chọn giao thức HTTP thay vì chọn HTTPS.

Đó là lý do tại sao khi bạn truy cập trang web Tuổi Trẻ Online (TTO), bạn không thấy bất kỳ văn bản màu xanh lá cây hoặc HTTPS trong thanh địa chỉ. Tất cả những gì bạn nhìn thấy trong hình dưới là một biểu tượng tài liệu trắng. Chứng tỏ rằng trang web này không sử dụng SSL, dữ liệu không được mã hóa.

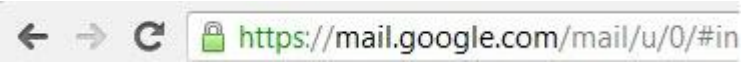
Vì vậy, nếu bạn gõ bất kỳ thông tin vào biểu mẫu trên trang web, dữ liệu đó sẽ không được mã hóa trên Internet và từ đó có khả năng có thể bị bắt gói tin và được đọc bởi bên thứ ba. Trong Google Chrome, nếu bạn bấm vào biểu tượng tài liệu, bạn sẽ nhận được một số thông tin chi tiết như dưới đây:

Có hai tab hiển thị: Permissions (Giấy phép) và Connection (Kết nối):

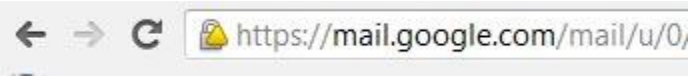
Tab Connection (Kết nối): Theo hình trên thì danh tính của trang web không được xác nhận. Điều này chứng tỏ TTO chưa mua chứng chỉ bảo mật cho trang web và vì thế TTO có thể được sở hữu bởi bất kỳ ai. Đó là lý do tại sao chúng ta không nên gõ bất kỳ thông tin nhạy cảm trên trang web không được mã hóa, nó sẽ công khai thông tin của bạn cho bất kỳ tổ chức nào.

Bây giờ bạn đã hiểu lý do tại sao không có văn bản màu xanh lá cây trong thanh địa chỉ?

Nếu bạn thường xuyên duyệt Gmail, trên thanh địa chỉ của bạn trông như thế này với một biểu tượng ổ khóa màu xanh lá cây khá đẹp và văn bản HTTPS màu xanh lá cây.

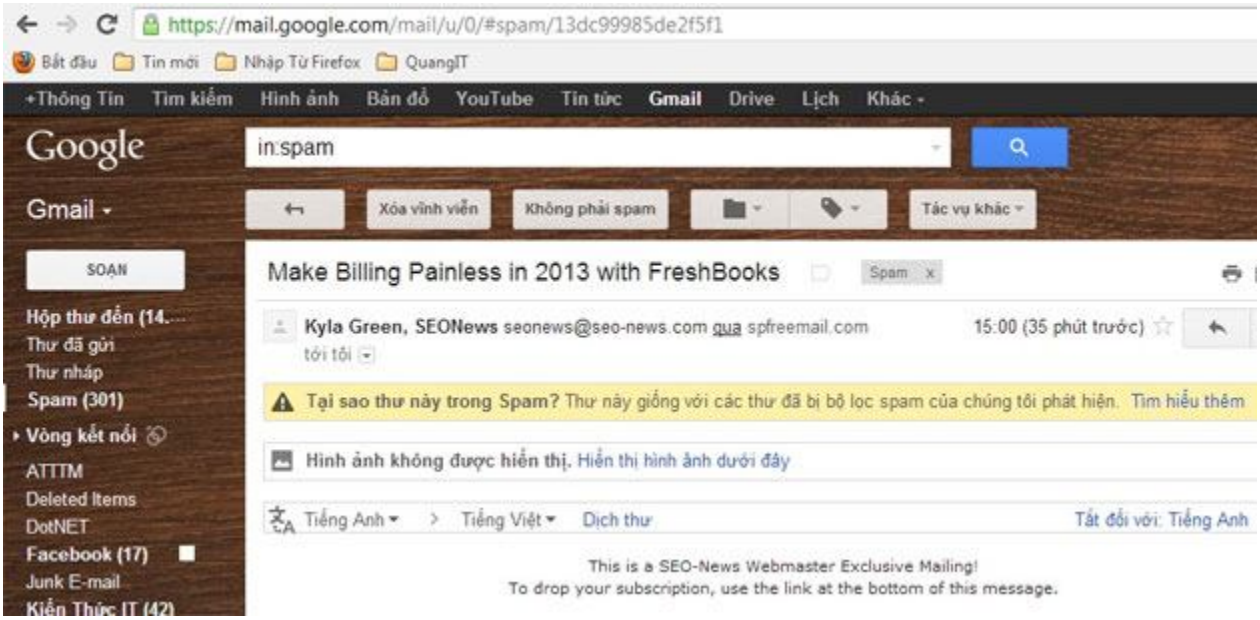


Tuy nhiên, sau một lúc biểu tượng chuyển sang màu xám với một hình tam giác màu vàng:



Biểu tượng này có nghĩa trang web đang sử dụng SSL mã hóa, nhưng một số nội dung trên trang này không an toàn (không mã hóa). Như vậy trang web này không an toàn?.

Ví dụ, trong Gmail, hình ảnh hiển thị trong email không chắc chắn là an toàn và do đó không được mã hóa. Đó là lý do tại sao bạn luôn luôn phải nhấp vào liên kết "*Luôn luôn hiển thị hình ảnh từ...*". Khi bạn nhấp vào liên kết, bạn sẽ nhận thấy sự thay đổi biểu tượng ổ khóa màu xanh lá cây thành hình tam giác màu xám. Do đó, Gmail là vẫn an toàn, nhưng một số nội dung trong email đó không an toàn.

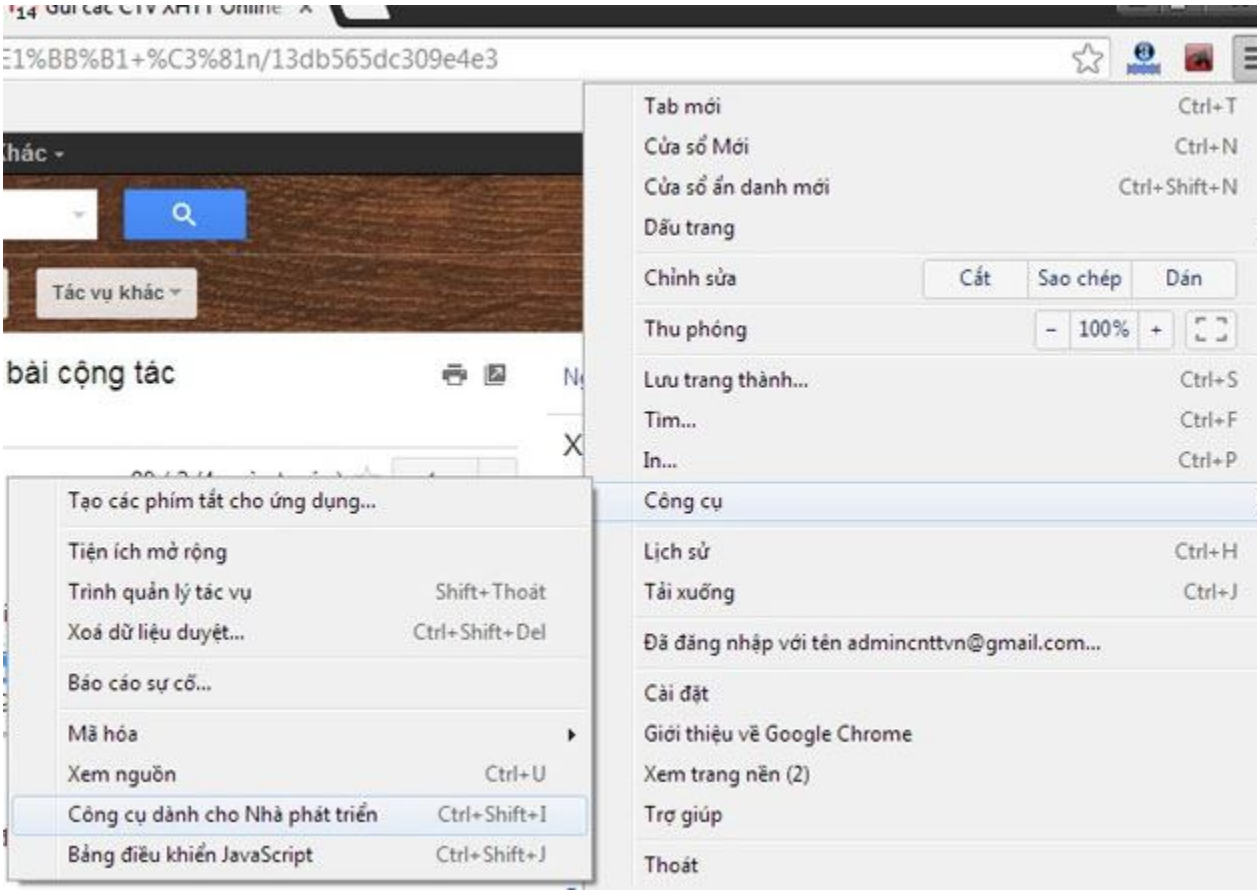


Tuy nhiên, nếu bạn gặp biểu tượng ổ khóa màu xám với dấu gạch chéo *"X"* màu đỏ ở vị trí trung tâm và đường gạch ngang văn bản HTTPS màu đỏ, biểu tượng này thực sự không an toàn, không đáng tin cậy.

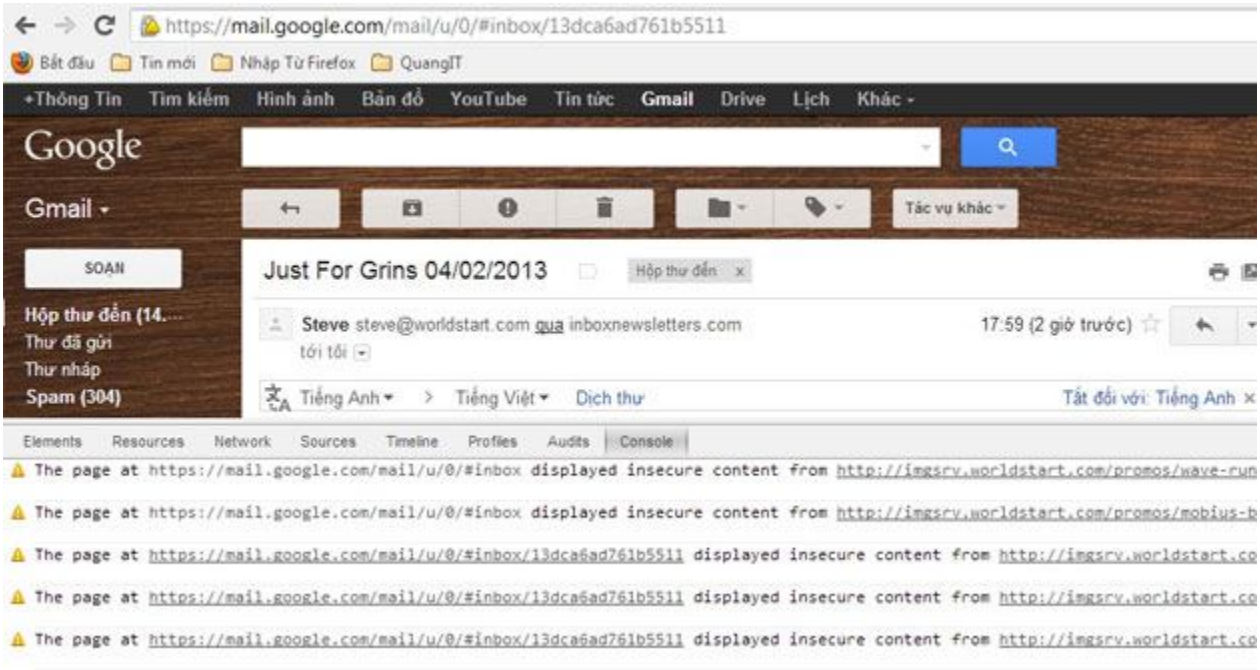
Đó có thể là do chứng chỉ bảo mật của trang web đang hết hạn sử dụng hoặc các nội dung liên quan đến Javascript không an toàn. Điều này thật sự có nguy cơ cao. Hình ảnh không được đánh giá nguy cơ cao vì thường không tương tác với người sử dụng. Tuy nhiên, nếu Javascript không an toàn, người dùng không nên nhập vào biểu mẫu vì dữ liệu truyền đi không an toàn.

Vậy làm thế nào biết nội dung trên trang đó không an toàn?

Bạn có thể kiểm tra xem trong Google Chrome. Click vào biểu tượng **Settings** ở phía trên bên phải, sau đó nhấn vào **Tools - Developer Tools** (Hoặc nhấn tổ hợp phím tắt **Ctrl + Shift + I**).



Khi đó, hãy nhấp vào **Tab Console** và bạn sẽ nhận được danh sách tất cả các cảnh báo hoặc lỗi như hình dưới đây.



Như bạn nhìn thấy từ hình trên, email từ Steve có một loạt các hình ảnh mà tôi đã quyết định hiển thị và những hình này được cho là không an toàn. Trong giao diện điều khiển, bạn có thể nhìn thấy những hình ảnh cụ thể thực tế đang gây ra các trang không an toàn.

Trên trang web mà bạn nhìn thấy với văn bản màu xanh lá cây và tên của công ty cũng màu xanh lá cây. Không có sự khác biệt trong mức độ mã hóa, an ninh, nó chỉ có một số hình ảnh tin cậy.

Như bạn có thể thấy, Apple Inc đã được xác minh bởi VeriSign Class 3 giấy chứng nhận mở rộng SSL Validation. Bạn cũng có thể thấy số lượng mã hóa (128 bit) và thông tin khác. Các ngân hàng thường có mã hóa 256 bit.

Bạn có thể tìm thêm thông tin về các cảnh báo bảo mật của Chrome và các biểu tượng **ở đây**.

Hy vọng bài viết này mang đến cho bạn một chút thông tin về giao thức HTTPS, cách làm việc SSL và làm thế nào để trình duyệt hiển thị thông tin đó vào thanh địa chỉ. Nó hiển thị hơi khác nhau trên mỗi trình duyệt, nhưng nhìn chung nó cũng tương tự.