HƯỚNG DẪN PHÁT HIỆN THƯ GIẢ MẠO

1. Phương thức tạo thư giả mạo của tin tặc

Thông thường khi soạn và gửi thư điện tử, người gửi thư chỉ biên soạn nội dung, tiêu đề thư (title), địa chỉ nơi nhận, lựa chọn các tệp tin đính kèm, các thông tin còn lại khác sẽ do máy chủ gửi thư tự động cập nhật như: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lại (Reply-To) và địa chỉhòm thư người gửi (from).

Để đánh lừa người nhận tin, bước đầu tin tặc sẽ tìm cách tự biên soạn thư điện tửvới các thông tin giả mạo về: địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi(from). Sau đó tin tặc sẽ tìm một máy chủ thư điện tử hoặc tự cài đặt một phần mềm gửi thư (MTA) không yêu cầu xác thực hòm thư người gửi để phát tán thư điện tử giảmạo tới người cần lừa đảo.

2. Cách phát hiện thư giả mạo

Trong nội dung thư điện tử gửi đến người nhận bao gồm các đầy đủ thông tin về: *địa chỉ IP của máy gửi thư; địa chỉ hòm thư nhận; địa chỉ hòm thư nhận phản hồi khi thư bị trả lại (Return-Path); địa chỉ hòm thư tiếp nhận thư trả lời (Reply-To) và địa chỉ hòm thư người gửi (from); nội dung thư; Tiêu đề thư; Các tệp tin đính kèm*. Nhưng trong chế độ hiển thị thông thường (mặc định) để đơn giản hóa giao diện, hầu hết các chương trình duyệt thư điện tử chỉ hiện các thông tin: *địa chỉ hòm thư tiếp nhận thư trả lời (Reply); Địa chỉ hòm thư người nhận; nội dung thư; tiêu đề thư; các tệp tin đính kèm và các thời gian liên quan*. Các thông tin chi tiết về nguồn gốc của thư được lưu trong phần đầu (header) của thư sẽ chỉ hiện thị chi tiết khi người nhận thư sử dụng các chức năng cho xem nguồn gốc (original) của thư hoặc xem nội dung phần đầu (header) của thư (Chú ý: đối với mỗi trình duyệt và hệ quản trị thư điện tử khác nhau sẽ có những cách khác nhau để xem nguồn gốc của thư điện tử, tuy nhiên tất cả các phần mềm trên đều hỗ trợ chức năng show original).

Qua phân tích các thư điện tử giả mạo đã gửi đến các cơ quan nhà nước trong thời gian vừa qua, có hai dấu hiệu chính để có thể phát hiện ra các thư giả mạo theo phương thức này là:

1. Khi mở xem nguồn gốc chi tiết của thư điện tử, địa chỉ hòm thư "Return-Path" không trùng với địa chỉ hòm thư người gửi đến (From). Hầu hết các thư điện tử được gửi từ các hệ thống thư điện tử của cơ quan nhà nước (có đuôi .gov.vn) đều có hai địa chỉ này trùng nhau.

2. Địa chỉ IP của máy chủ gửi thư không trùng với địa chỉ IP của hệ thống thư điện tử thật nơi bị giả mạo là gửi thư điện tử. Hiện nay, các địa chỉ IP giả mạo này thường có nguồn gốc từ nước ngoài trong khi địa chi IP các hệ thống cơ quan nhà nước thường có địa chỉ IP trong nước.

Vì vậy để phát hiện thư giả mạo chúng ta cần xem thông tin chi tiết về nguồn gốc của thư. Các thông tin chính cần kiểm tra là: Địa chỉ IP máy gửi thư, thông tin "Return-Path".

- Khi nhận thư từ địa chỉ thư điện tử công vụ (là thư có đuôi @quangninh.gov.vn) mà không có địa chỉ IP máy chủ gửi thư là 123.30.50.140 thì đó là thư giả mạo.

  Ví dụ nếu trong chi tiết nguồn gốc thư có thông tin như thế này thì thư không phải là giả mạo:

  *Received: from mail.quangninh.gov.vn ([**123.30.50.140**]) by*

  mail.quangninh.gov.vn ([123.30.50.140]) with mapi;

- Đối với thư nhận được từ các hệ thống thư khác, nếu "Return-Path" không trùng với địa chỉ hòm thư người gửi đến (From) thì đó là thư giả mạo.

3. Cách xem thông tin chi tiết nguồn gốc của thư điện tử công vụ

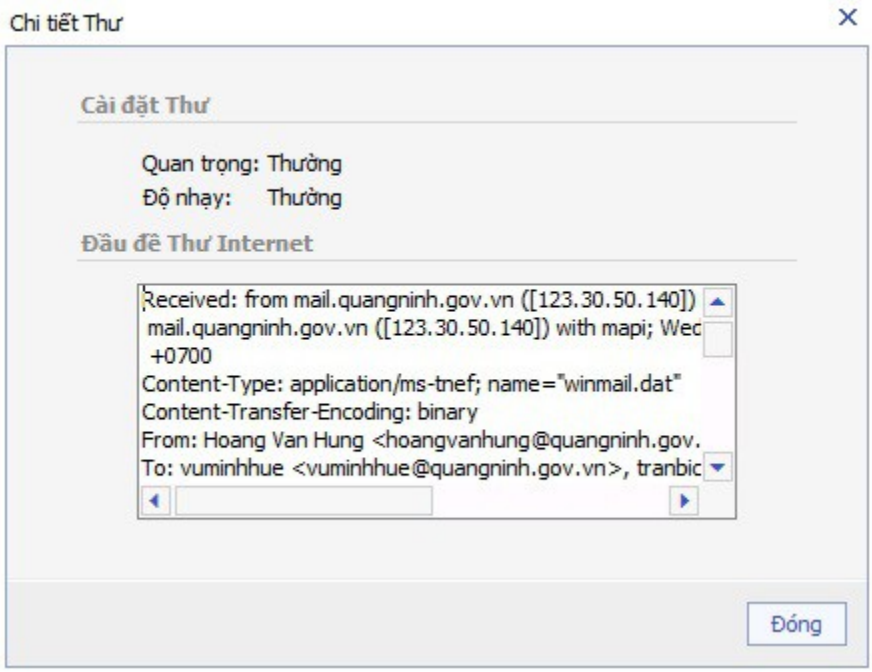
3.1. Sử dụng webmail

Vì Thư điện tử được xây dựng trên nền tảng của Microsoft nên chỉ sử dụng trình duyệt Internet Explorer mới có thể nhìn thấy nội dung chi tiết nguồn gốc thư. Các bước làm như sau:

Bước 1: Click đúp vào thư cần xem thông tin.

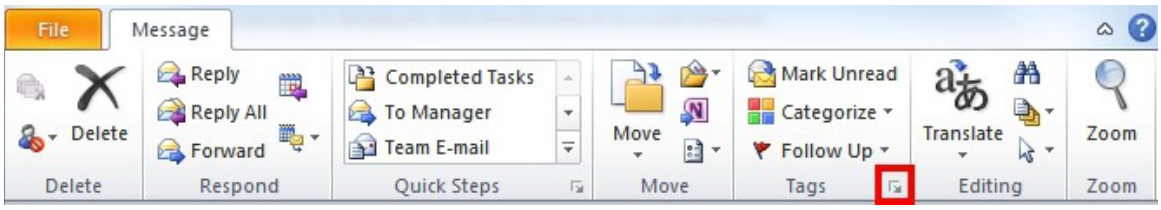
Bước 2: Click vào icon " Chi tiết thư" như trong hình bên dưới:

Thông tin chi tiết nguồn gốc thư sẽ hiện ra như sau:

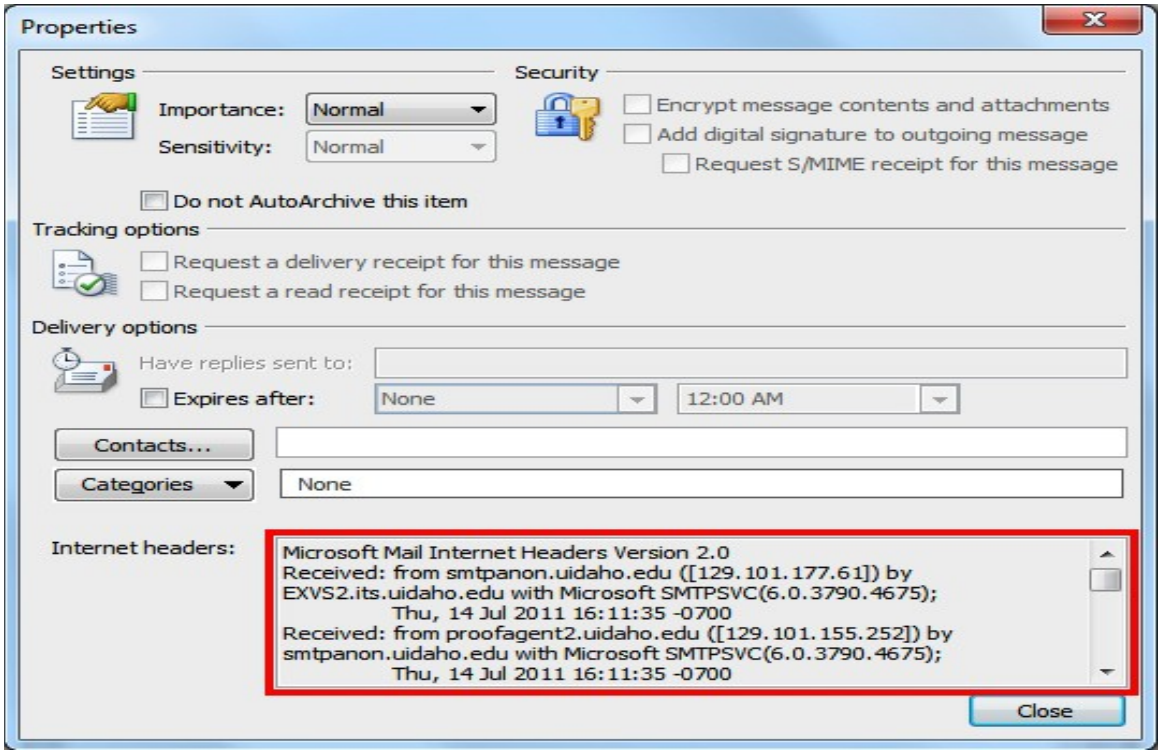


3.2. Sử dụng phần mềm Microsoft Outlook 2010 và các phiên bản mới hơn

Kích đúp vào tin nhắn để mở ra cửa sổ mới. Từ thanh công cụ -> **tab Message** -> kích vào ô nhỏ có hình mũi tên trong khung **Tags** hoặc **Options**

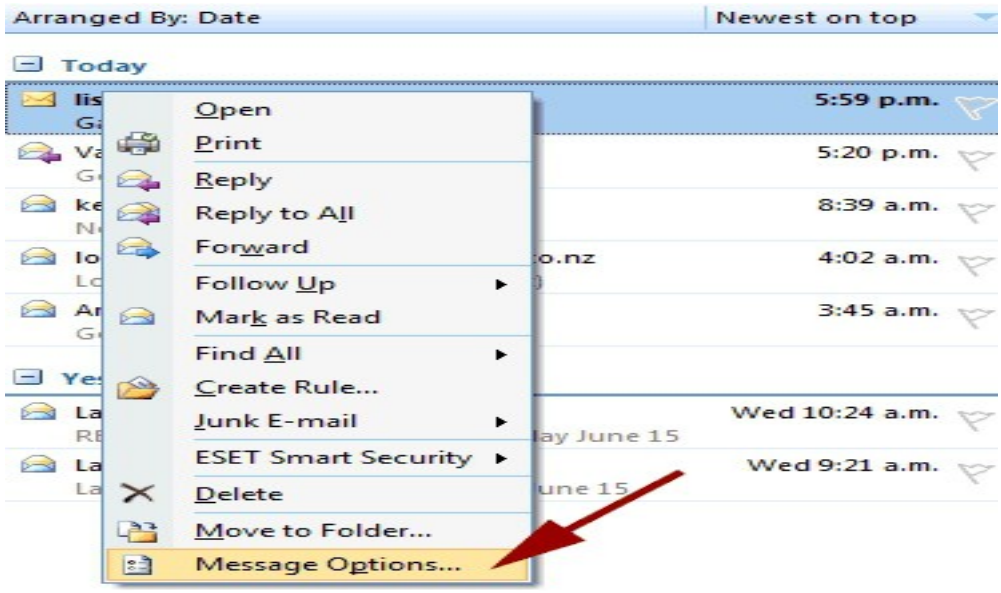


Cửa sổ Properties mở ra và hiển thị phần tiêu đề thư:



3.3. Sử dụng phần mềm Microsoft Outlook các phiên bản trước 2010

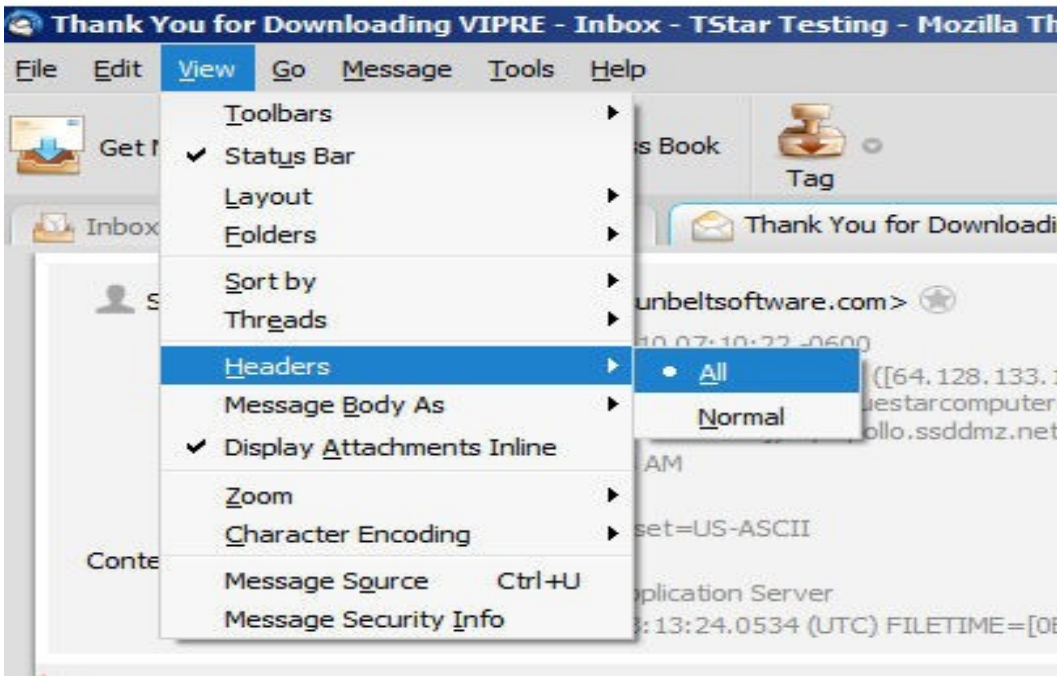
Kích phải vào tin nhắn muốn hiển thị và chọn **Message Options**



Sau đó cửa sổ Properties chứa tiêu đề thư sẽ được hiển thị.

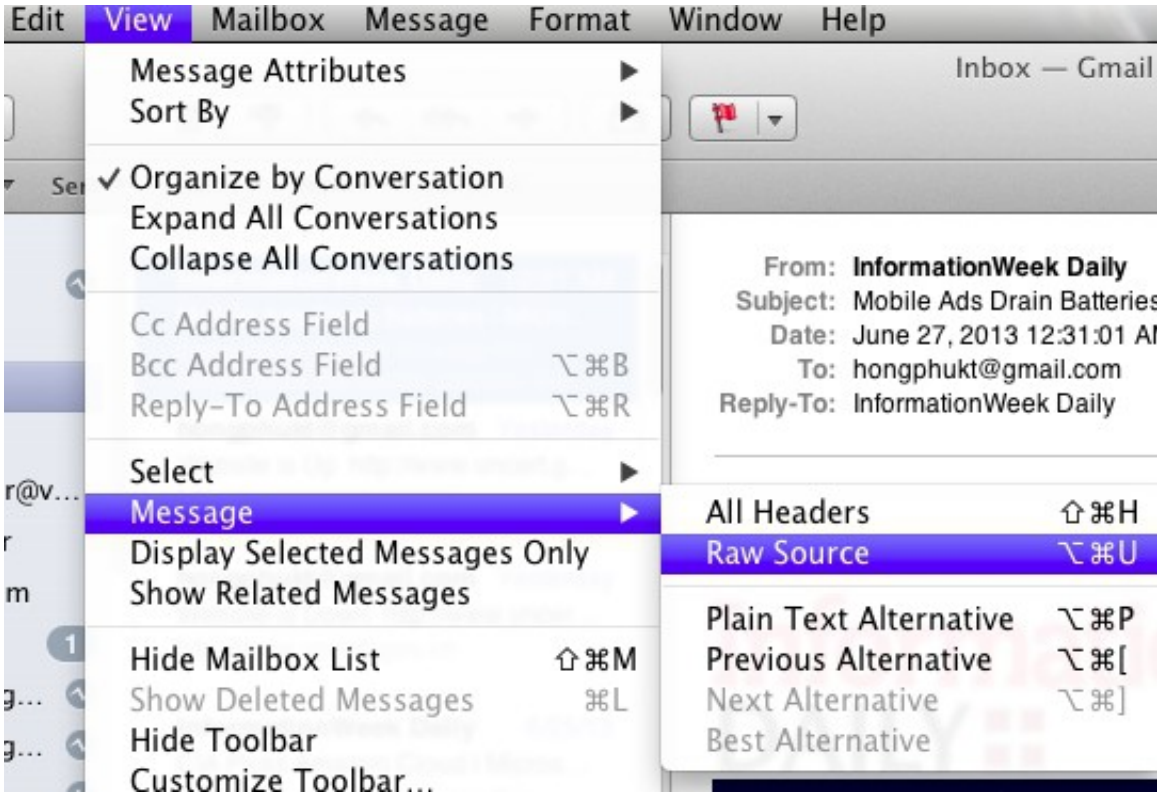
3.4. Sử dụng phần mềm Thunder Bird

Mở tin nhắn chọn **"View"** sau đó chọn **"Message Source"** hoặc **Headers -> All**:



3.5. Sử dụng phần mềm Apple Mail

Mở tin nhắn chọn **"View"** trên thanh menu sau đó chọn **"Message"**, tiếp đó chọn "**All Header"** hoặc "**Raw Source** "



Tài liệu có tham khảo từ website: http://vncert.gov.vn.