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 chỉ hòm thư người gửi (from).

Để đánh lừa người nhận tin, bước đầu tin tặc sẽ tìm cách tự biên soạn thư điện tử với 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 giả mạo tới người cần lừa đảo.

2. Tìm hiểu nguồn gốc thật phát tán của thư điện tử

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 như: địa chỉ IP của máy gửi thư; 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) 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). Cách xem nguồn gốc thư điện tử của một số hệ thống thư điện tử phổ biến sẽ được trình bày trong Phụ lục A

3. Phát hiện thư giả mạo

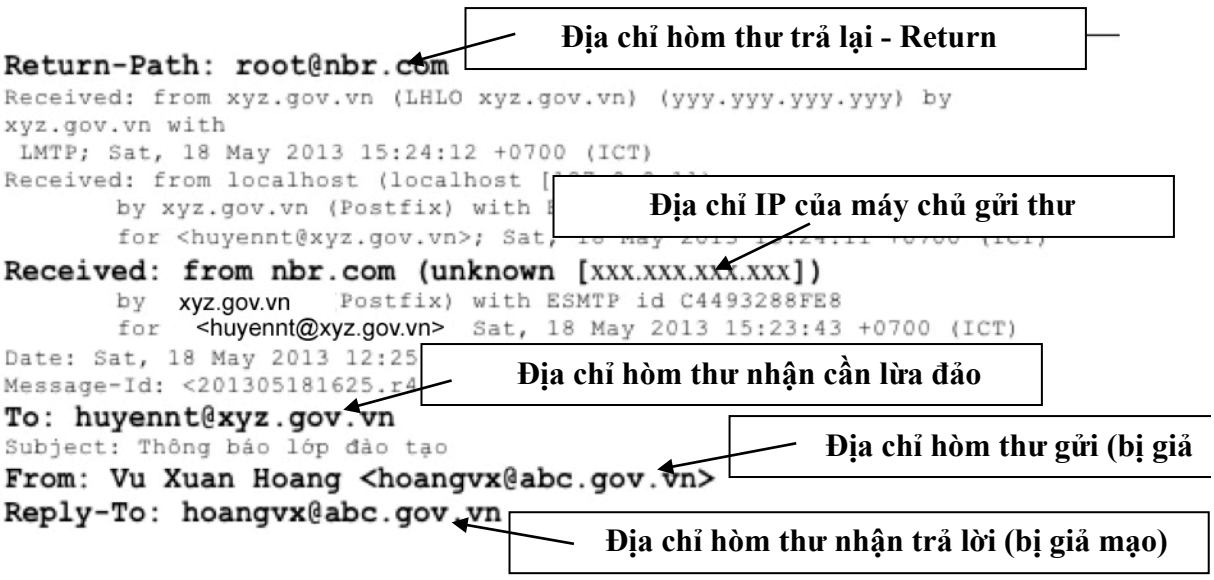
Qua phân tích các thư điện tử giả mạo đã gửi đến các cơ quan nhà nước trong thời gian vừa qua, có hai dấu hiệu chính để có thể phát hiện ra các thư giả mạo theo phương thức này là:

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.

Ví dụ minh họa :

Dưới đây là ví dụ minh họa một thư điện tử giả mạo ông Vũ Xuân Hoàng có địa chỉ thư điện tử là hoangvx@abc.gov.vn được tin tặc gửi tới hòm thư của chị Nguyễn Thanh Huyền có địa chỉ huyennt@xyz.gov.vn. Tin tặc tạo ra thư giả mạo ông Vũ Xuân Hoàng có tiêu đề là "Thông báo lớp đào tạo" với các địa chỉ hòm thư gửi, và hòm thư nhận là hoangvx@abc.gov.vn, hòm thư trả lại là root@nbr.com. Sau đó tin tặc sử dụng máy gửi thư có địa chỉ IP xxx.xxx.xxx.xxx để gửi thư giả mạo đã soạn tới hòm thư của chị Nguyễn Thanh Huyền có địa chỉ huyennt@xyz.gov.vn.



4. Báo cáo khi nhận được thư giả mạo

Khi phát hiện được thư giả mạo, đề nghị gửi thư giả mạo theo hình thức dưới dạng tệp tin đính kèm (attachment hoặc forward as attachment) tới địa chỉ antoanthudientu@report.vncert.vn của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam. Cách gửi thư giả mạo dưới dạng tập tin đính kèm sẽ được trình bày trong Phụ lục B.

Để gửi thông tin về cho chúng tôi xin vui lòng làm theo mẫu sau sau:

Địa chỉ: antoanthudientu@report.vncert.vn

Tiêu đề: Báo cáo thư giả mạo

Nội dung:

Báo cáo thư giả mạo.

Tên người gửi: *Nguyễn Văn A*

Địa chỉ Email liên lạc:*nva@zyx.gov.vn*

Số điện thoại liên hệ: *09xxxxxxx*

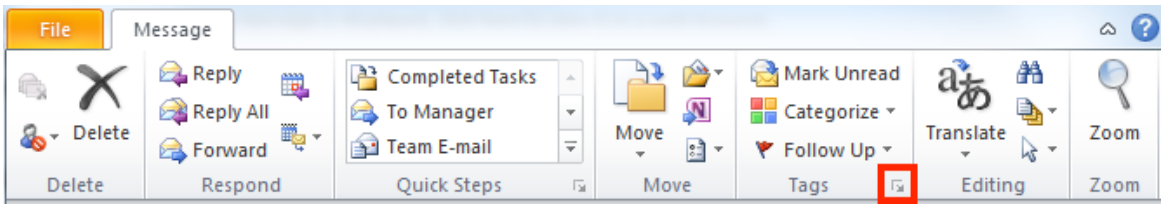
Thông tin chi tiết về vấn đề: *Tôi nhận được email nghi vấn giả mạo từ địa chỉ XXX với nội dung lừa đảo để tôi gửi thông tin về lãnh đạo cơ quan....*

Tập tin đính kèm chứa nội dung nguyên bản (chứa đầy đủ phần đầu của thư điện tử): msg001.mail

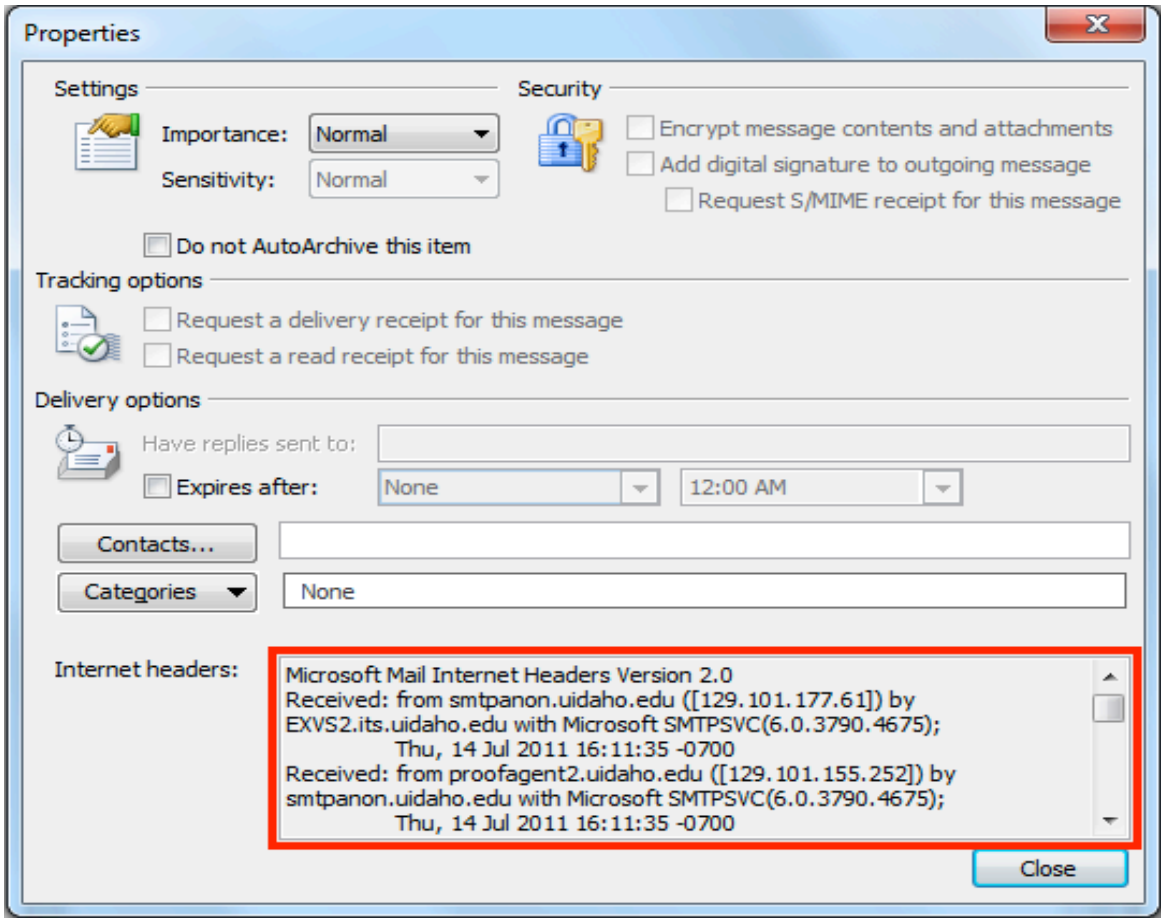
Phụ lục A : Hướng dẫn hiển thị tiêu đề của thư điện tử

1. 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**

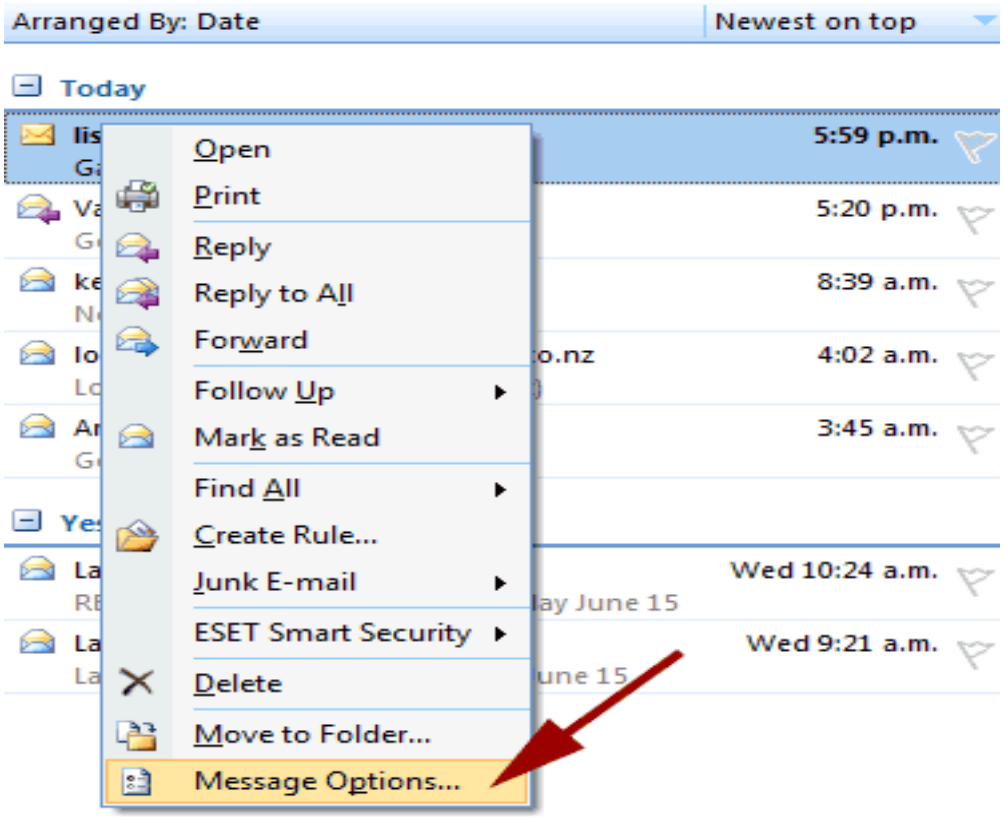


Cửa sổ **Properties** mở ra và hiển thị phần tiêu đề thư:



2. Phần mềm Microsoft Outlook các phiên bản trước 2010:

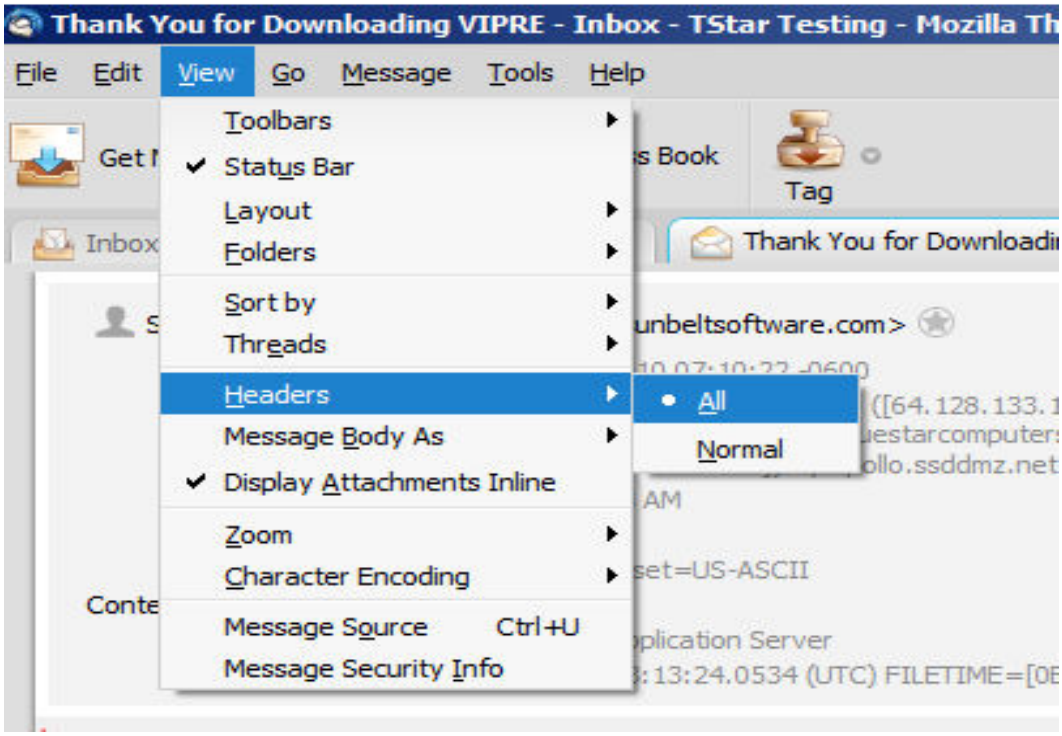
Kích phải vào tin nhắn muốn hiển thị và chọn **Message Options**



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

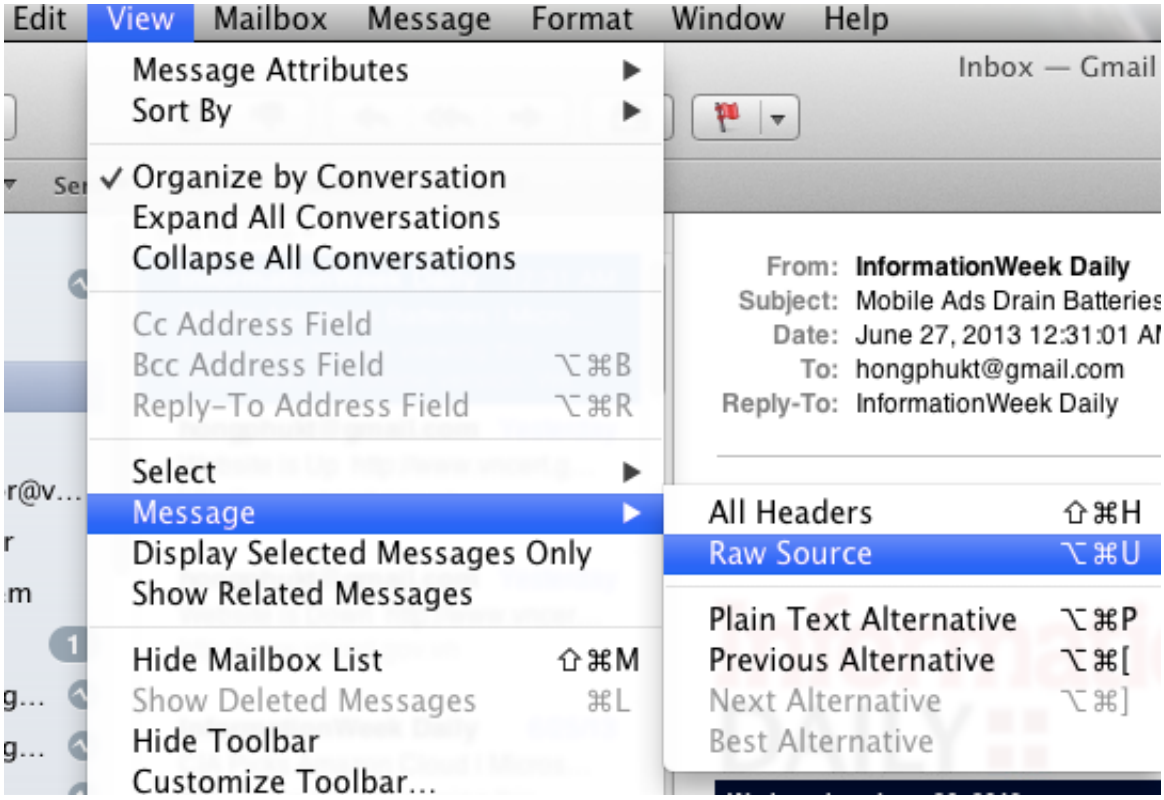
3. Phần mềm Thunder Bird :

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



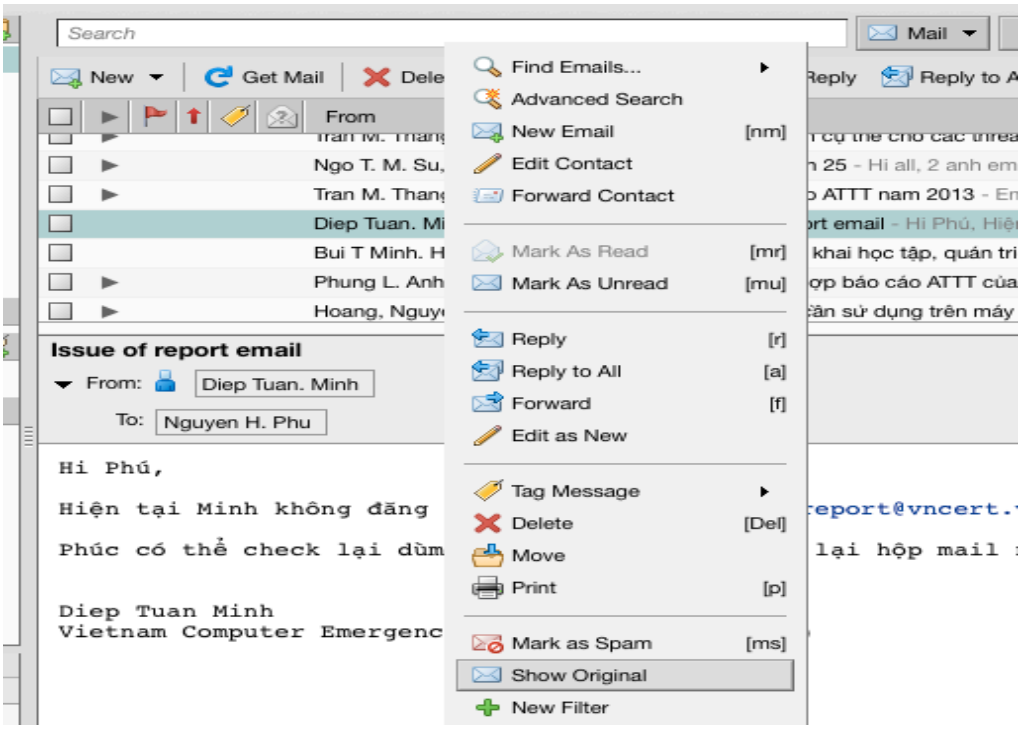
4. Phần mềm Apple Mail :

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



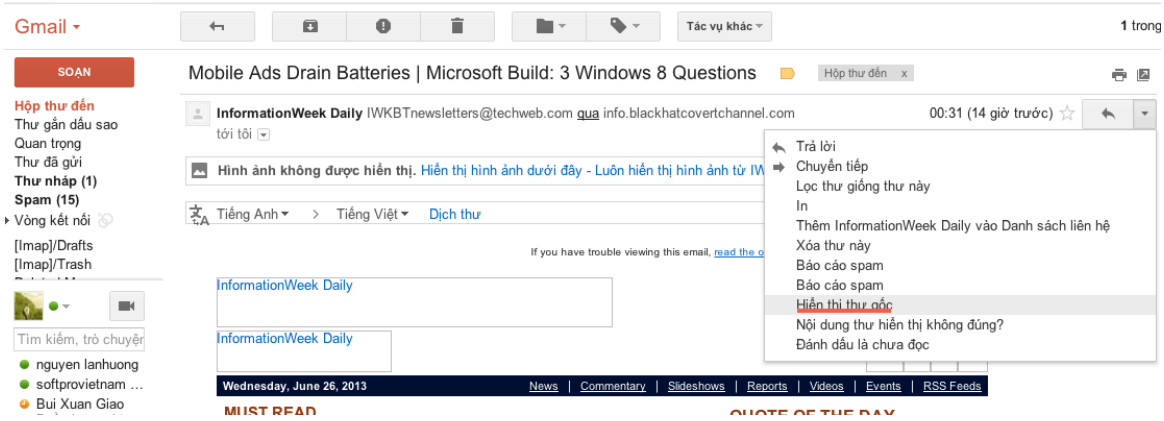
5. Webmail với hệ quản trị email Zimbra:

Ấn chuột phải vào thư điện tử cần xem. Lựa chọn mục **Show Original**:



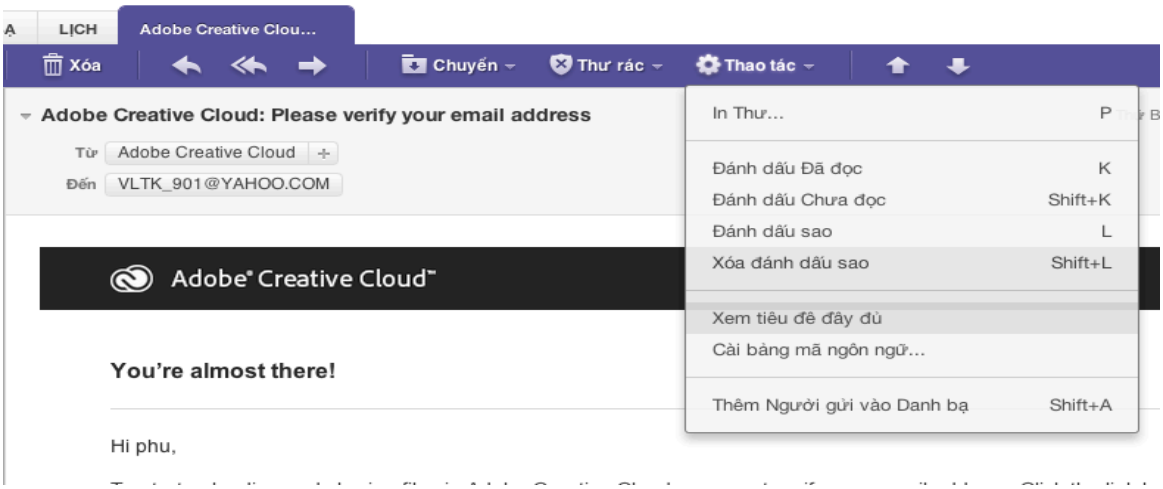
6. Đối với Webmail của Gmail

Sau khi mở email cần hiển thị ta kích vào mũi tên nhỏ bên phải và kích vào "**hiển thị thư gốc**":



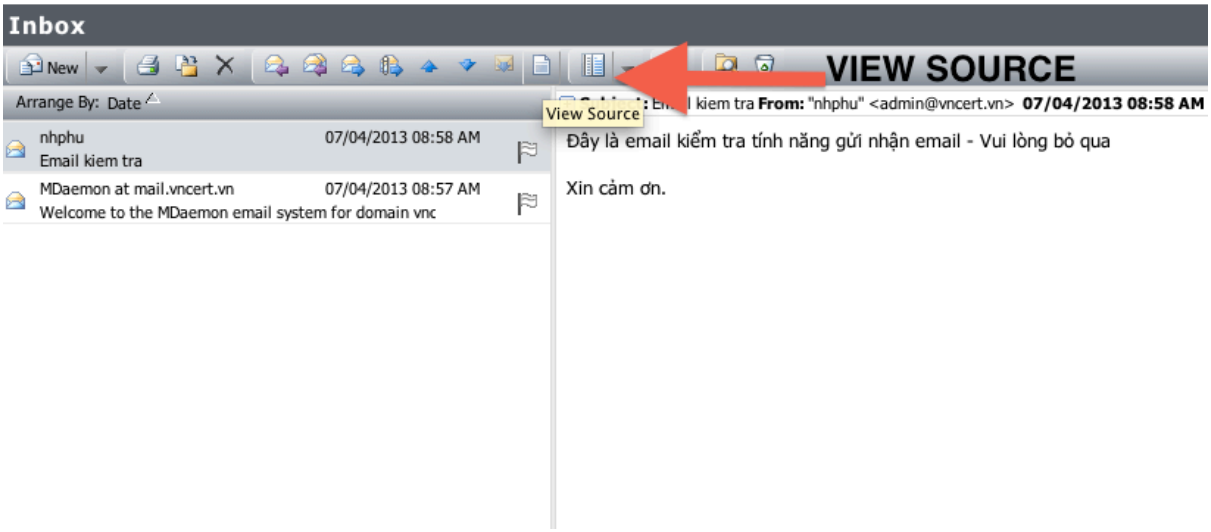
7. Đối với Webmail của Yahoomail

Thực hiện lựa chọn tin nhắn cần hiển thị. Chọn nút "**Thao tác**" trên thanh công cụ -> "**Xem tiêu đề đầy đủ**" để hiển thị tiêu đề thư:



8. Đối với Webmail của mail Mdaemon 13.5

Lựa chọn tin nhắn cần hiển thị. Kích vào mục "**View Source**" trên thanh công cụ để hiển thị nội dung gốc của tin nhắn.



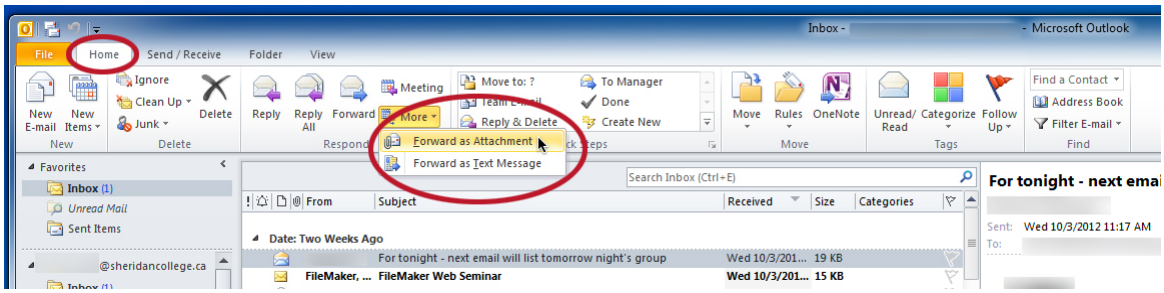
Sau khi click vào thanh công cụ sẽ hiển thị phần nội dung gốc của thư điện tử cần kiểm tra

```
Return-path: <admin@vncert.vn>
Received: from WorldClient by mail.vncert.vn (MDaemon PRO v13.5.1 trial)
        with ESMTP id md50000000001.msg
        for <nhphu@vncert.vn>; Thu, 04 Jul 2013 08:58:18 +0700
Authentication-Results: mail.vncert.vn
        auth=pass smtp.mail=admin@vncert.vn
X-Spam-Processed: mail.vncert.vn, Thu, 04 Jul 2013 08:58:18 +0700
        (not processed: message from trusted or authenticated source)
X-Authenticated-Sender: admin@vncert.vn
X-Rcpt-To: nhphu@vncert.vn
X-MDRcpt-To: nhphu@vncert.vn
X-Return-Path: admin@vncert.vn
X-Envelope-From: admin@vncert.vn
X-MDaemon-Deliver-To: nhphu@vncert.vn
Received: by vncert.vn via WorldClient with HTTP;
        Thu, 04 Jul 2013 08:58:13 +0700
Date: Thu, 04 Jul 2013 08:58:13 +0700
From: "nhphu" <admin@vncert.vn>
To: nhphu@vncert.vn
```

Phụ lục B : Hướng dẫn gửi thư giả mạo dưới dạng tệp

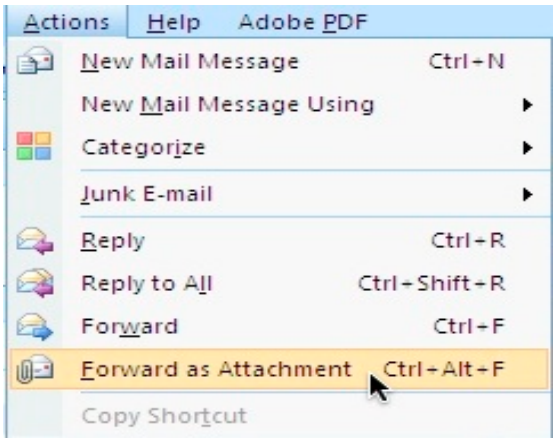
1. Đối với Outlook 2010

Lựa chọn tin nhắn muốn gửi đi. Lựa chọn tab "**Home**" trên thanh công cụ. Trong mục "**Respond**" chọn "**More**"->"**Forward as Attachment**"



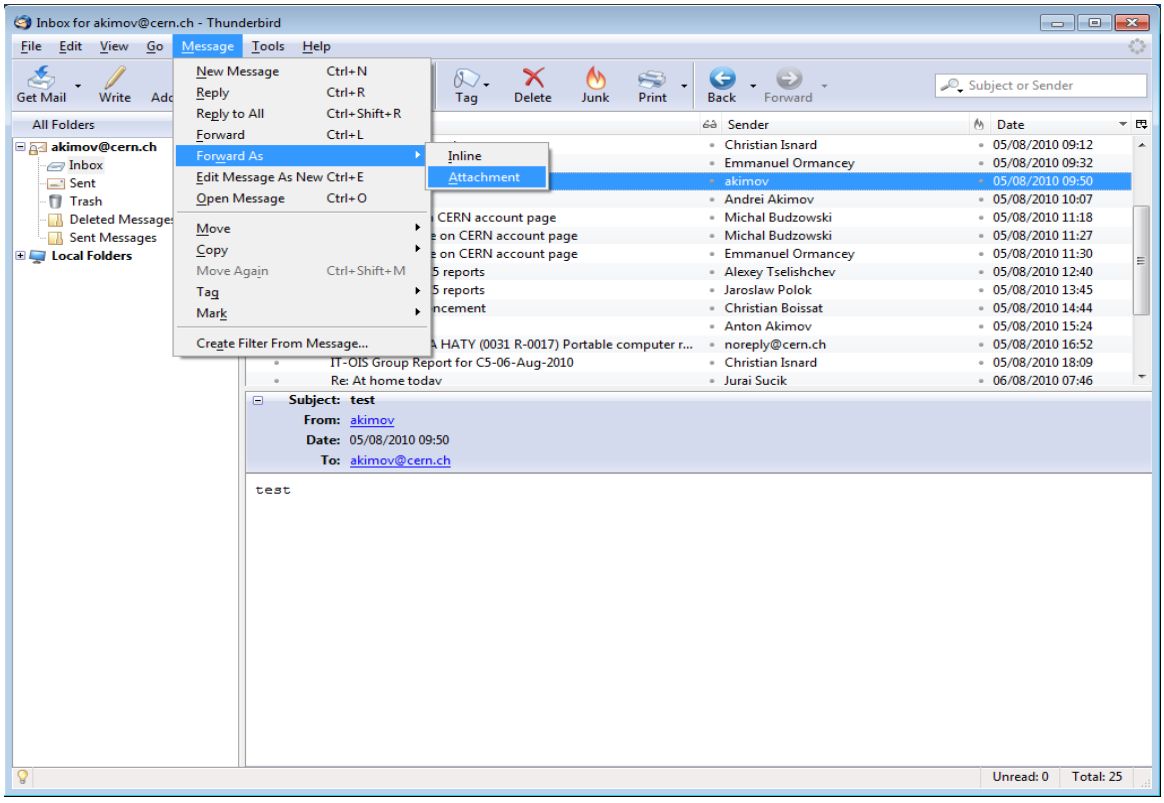
2. Đối với Outlook 2007

Lựa chọn tin nhắn muốn gửi. Lựa chọn "**Action**" menu và kích vào "**Forward as Attachment**"



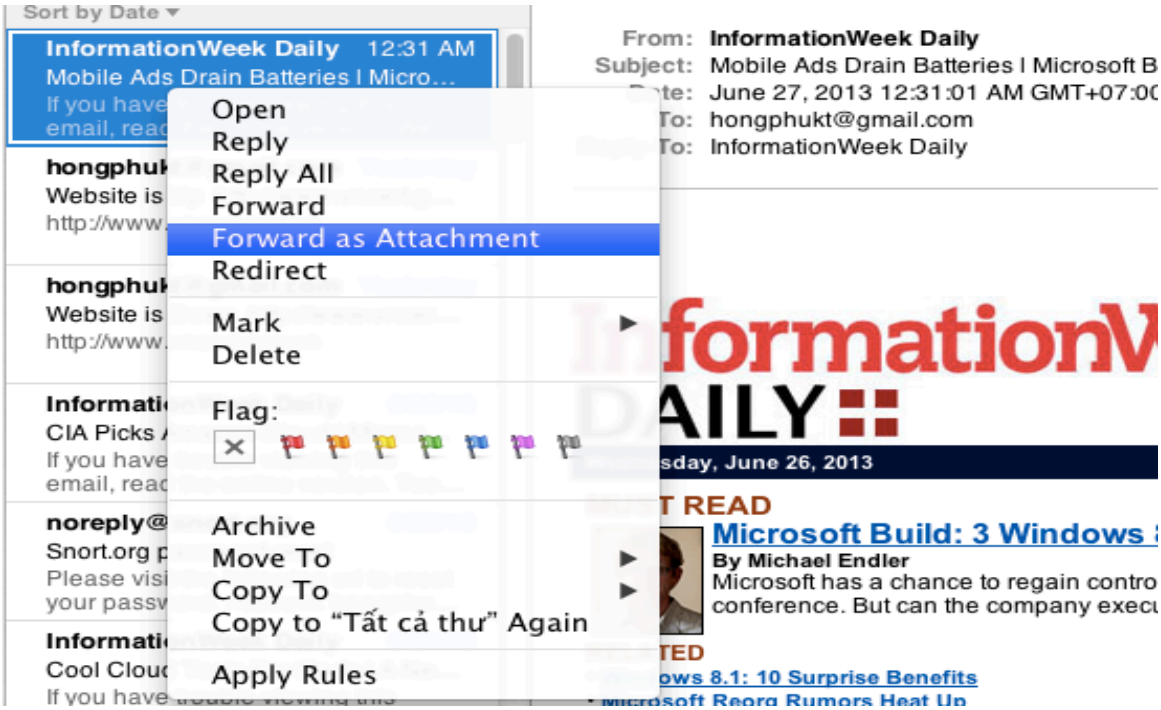
3. Đối với Thurnderbird

Lựa chọn tin nhắn, menu "**Message**" -> **Foward As** -> **Attachment**.



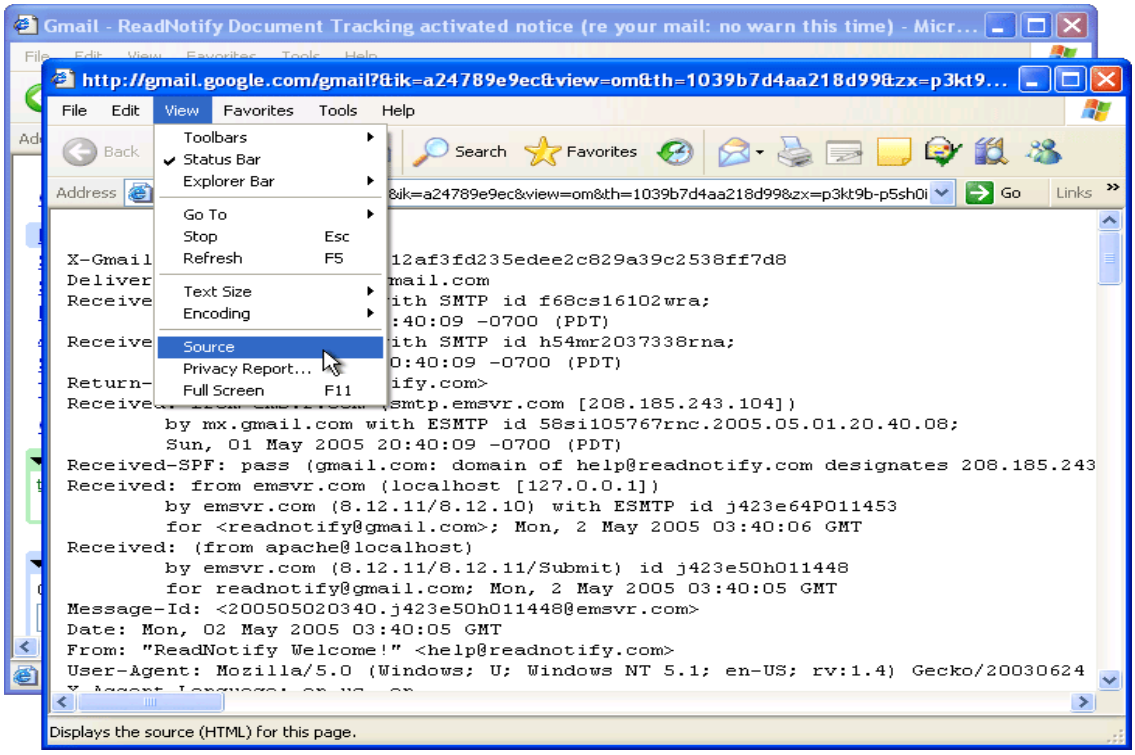
4. Đối với Apple Mail

Click chuột phải vào tin nhắn muốn gửi và lựa chọn "**Forward as Attachment**"



5. Đối với Gmail và Yahoo

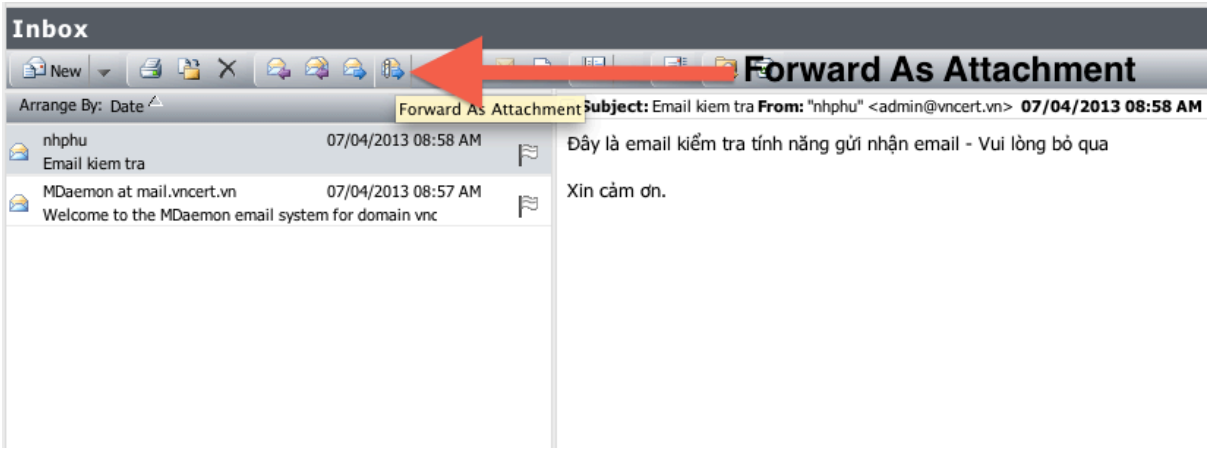
Ta cần phải hiển thị thư gốc ra như hướng dẫn 6 và 7 ở Phụ lục A và lưu chúng lại thành một tập tin dạng văn bản.



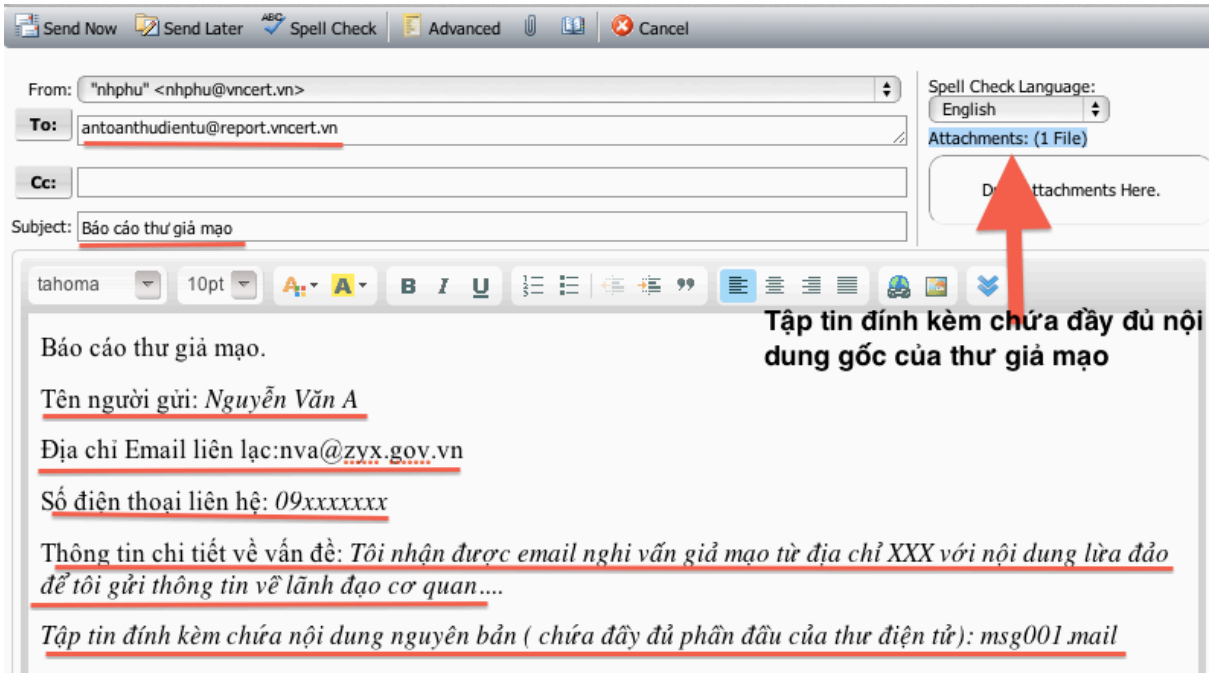
Sau đó thực hiện gửi email đính kèm tập tin văn bản đó cho chúng tôi.

6. Webmail của Mdaemon 13.5

Mở tin nhắn nghi vấn cần gửi đi và kích vào nút "**Forward As Attachment**" trên thanh công cụ:



Một giao diện soạn thư sẽ được hiển thị. Ta cần điền đầy đủ thông tin theo như mẫu ở phần 4 và gửi về hòm thư antoanthudientu@report.vncert.vn


Send Now
Send Later
Spell Check
Advanced
Cancel
From: "nhphu" <nhphu@vncert.vn>
To: antoanthudientu@report.vncert.vn
Cc:
Subject: Báo cáo thư giả mạo
Spell Check Language:
English
Attachments: (1 File)
Attachments Here.
tahoma
10pt
Tập tin đính kèm chứa đầy đủ nội dung gốc của thư giả mạo
Báo cáo thư giả mạo.
Tên người gửi: Nguyễn Văn A
Địa chỉ Email liên lạc:nva@zyx.gov.vn
Số điện thoại liên hệ: 09xxxxxxx
Thông tin chi tiết về vấn đề: Tôi nhận được email nghi vấn giả mạo từ địa chỉ XXX với nội dung lừa đảo để tôi gửi thông tin về lãnh đạo cơ quan....
Tập tin đính kèm chứa nội dung nguyên bản (chứa đầy đủ phần đầu của thư điện tử): msg001.mail