NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

CỤC CÔNG NGHỆ TIN HỌC

HƯỚNG DẪN PHÁT HIỆN THƯ ĐIỆN TỬ GIẢ MẠO

Hà Nội 07/2013

MỤC LỤC

I. MỤC ĐÍCH:

Tài liệu này được xây dựng nhằm hướng dẫn cán bộ của các Vụ, Cục, Đơn vị trực thuộc Ngân hàng Nhà nước và các Ngân hàng Nhà nước chi nhánh tỉnh, thành phố phòng và phát hiện thư điện tử giả mạo.

II. NỘI DUNG HƯỚNG DẪN:

1. Định dạng của một thư điện tử.

Một thư điện tử bao gồm 2 thành phần chính là:

- **Phần đầu thư (Message Header):** bao gồm một số các trường thông tin cơ bản sau:
  - **From**: Địa chỉ hòm thư **người gửi**.
  - **To**: Địa chỉ hòm thư **người nhận**.
  - **Return-Path**: địa chỉ hòm thư sẽ nhận thư trả lại trong trường hợp thư gửi không đi được. Trường này là được máy chủ thư điện tử tự động chèn vào phần đầu thư, do đó **Kẻ Tin Tặc** không thể sửa đổi trường thông tin này. **Một thư điện tử chắc chắn bị giả mạo nếu trường Return-Path khác trường From.**
  - **Reply-To**: địa chỉ hòm thư sẽ nhận thư trả lời của **người nhận** trả lời lại thư của **người gửi**.
  - **Received:** trường này gồm nhiều giá trị, mỗi giá trị trên một dòng cho biết thư điện tử được nhận từ máy chủ nào gửi đến và máy chủ nào nhận thư điện tử này. Thứ tự chuyển thử điện tử giữa các máy chủ được liệt kê từ dưới lên trên. Do đó, giá trị **Received trên cùng** của Phần đầu thư cho biết thông tin máy chủ thư điện tử nhận cuối cùng và giá trị **Received dưới cùng** của Phần đầu thư là cho biết thông tin máy chủ thư điện tử của người gửi.

Ví dụ:

Received: *from* ***smtp1.s.gov.vn (10.1.1.16)*** *by s.gov.vn* ***(10.1.1.15)***

with Microsoft SMTP Server (TLS) id 14.1.355.2; Wed, 17 Jul 2013 01:05:14

+0700

Received: *from em-sj-81.mktomail.com* ***([199.15.215.81])*** *by* ***smtp1.sbv.gov.vn*** *with ESMTP; 17 Jul 2013 01:05:12 +0700*

Đối với phần đầu thư như ví dụ trên thì **199.15.215.81** là địa chỉ IP máy chủ thư điện tử người gửi và tại thời điểm này thư điện tử được nhận bởi máy chủ thư điện tử **smtp1.sbv.gov.vn** có địa chỉ IP **10.1.1.16**.

- **Subject:** tiêu đề thư.
- **Attachment**: các tệp tin được người gửi đính kèm theo thư điện tử.

- **Phần nội dung thư (Message Body):** là nội dung của thư điện tử.

Tuy nhiên, trong chế độ hiển thị thông thường của một số trình gửi và nhận thư điện tử, **người nhận** thư chỉ thấy các thông tin: **From, To, Subject, Message Body, Attachment.**

2. Phương pháp phát hiện thư điện tử giả mạo.

Qua phân tích các thư điện tử giả mạo trong thời gian vừa qua, có **2 dấu hiệu chính** để phát hiện thư giả mạo bằng cách xem **Phần đầu thư** của một thư điện tử:

- Giá trị trường **From** và **Return-Path** khác nhau: Kẻ Tin Tặc thay trường **From** bằng địa chỉ hòm thư của người cần giả mạo.
- **Địa chỉ IP máy chủ thư điện tử của người gửi** khi kiểm tra qua website **http://whois.domaintools.com** thì **địa chỉ IP máy chủ thư điện tử của người gửi** (OrgName hoặc org-name) **không phải là tổ chức của người gửi (From).**

Ngoài ra 2 dấu hiệu chính trên Người nhận cần kiểm tra cẩn thận:

- Giá trị trường **Reply-To**: Kẻ Tin Tặc **có thể** thiết lập trường **Reply-To** bằng địa chỉ hòm thư của Kẻ Tin Tặc. Khi đó **Reply-To** sẽ khác **From, Return-Path.**
- Kẻ Tin Tặc tạo và sử dụng một địa chỉ hòm thư người gửi gần giống với địa chỉ hòm thư của người cần giả mạo.

Ví dụ:

- Địa chỉ hòm thư Kẻ Tin Tặc là KeTinTac@gmail.com

- Địa chỉ hòm thư người cần giả mạo là BiGiaMao@sbv.gov.vn

- Địa chỉ hòm thư người nhận là BiLua@sbv.gov.vn

- Địa chỉ IP máy chủ gửi thư điện tử người gửi (Kẻ Tin Tặc) là **188.158.9.23,** kiểm tra trên **http://whois.domaintools.com** thì địa chỉ IP này là của tổ chức **Neda Gostar Saba Data Transfer Company Private Joint Stock**, không phải của **Ngân hàng Nhà nước Việt Nam**.

Khi đó Kẻ Tin Tặc bằng cách nào đó sẽ thực hiện gửi một thư điện tử có Phần đầu thư có nội dung sau:

Received: *from HQ-EXCH02.SBV.VN (10.1.3.16) by HQ-EXCH01.SBV.VN (10.1.3.15) with Microsoft SMTP Server (TLS) id 14.1.355.2; Tue, 16 Jul 2013 16:55:39 +0700*

Received: *from mailmig01.sbv.gov.vn (10.1.3.24) by HQ-EXCH02.SBV.VN (10.1.3.16) with Microsoft SMTP Server id 14.1.355.2; Tue, 16 Jul 2013 16:55:38 +0700*

Received: *from smtp1.sbv.gov.vn ([172.16.2.30]) by mailgw2.sbv.gov.vn (Lotus Domino Release 8.5.1FP4) with ESMTP id 2013071616553829-11195 ;Tue, 16 Jul 2013 16:55:38 +0700*

Received: *from unknown (HELO [**188.158.9.23**]) ([188.158.9.23]) by smtp1.sbv.gov.vn with ESMTP; 16 Jul 2013 16:55:34 +0700*

Received: *from **188.158.9.23** (HELO sbv.gov.vn) by sbv.gov.vn (CommuniGate Pro SMTP 5.2.3) with ESMTPA id 692796901 Tue, 16 Jul 2013 13:30:11 +0330*

Return-Path: KeTinTac@gmail.com

From: BiGiaMao@sbv.gov.vn

Reply-To: BiGiaMao@sbv.gov.vn

To: BiLua@sbv.gov.vn

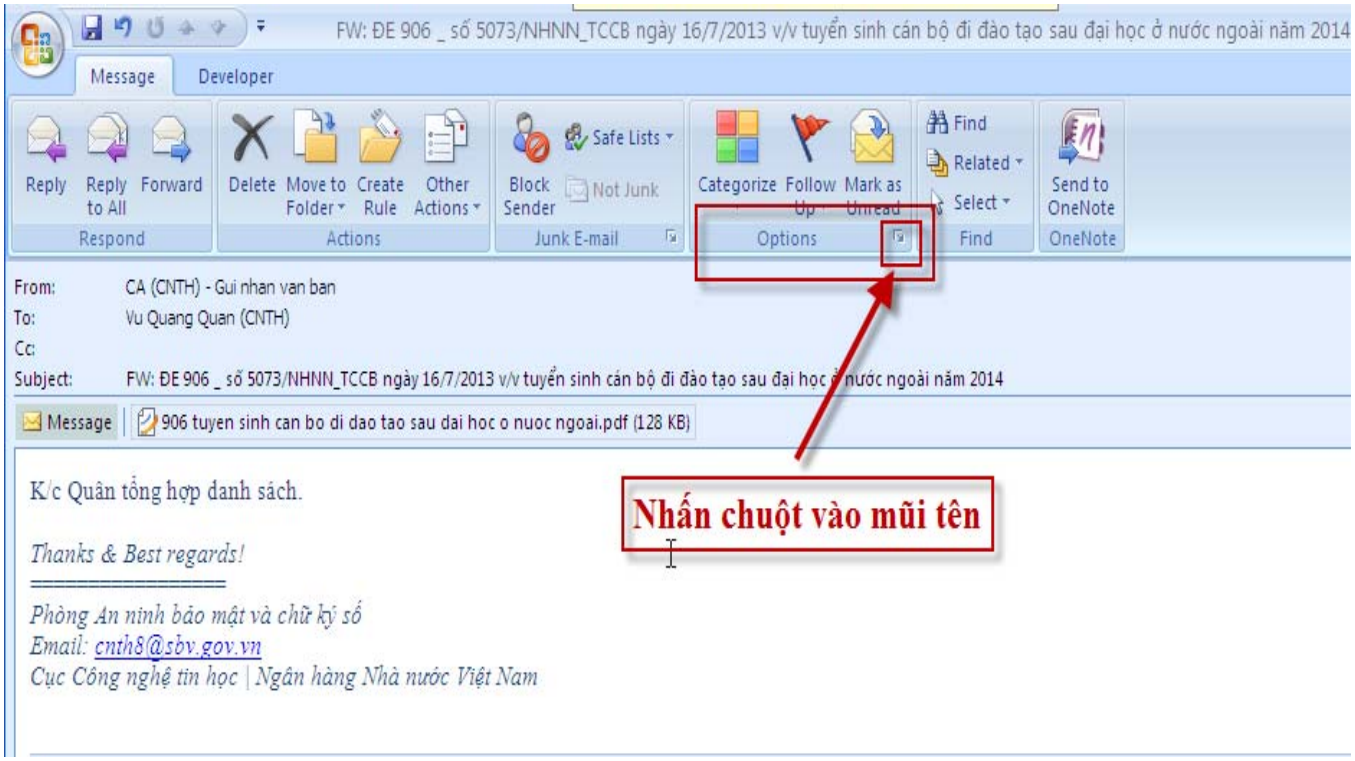
Subject: Em ơi password thẻ ATM Đông Á, Em mới đổi là gì nhỉ?

3. Hướng dẫn xem Phần đầu thư của một thư điện.

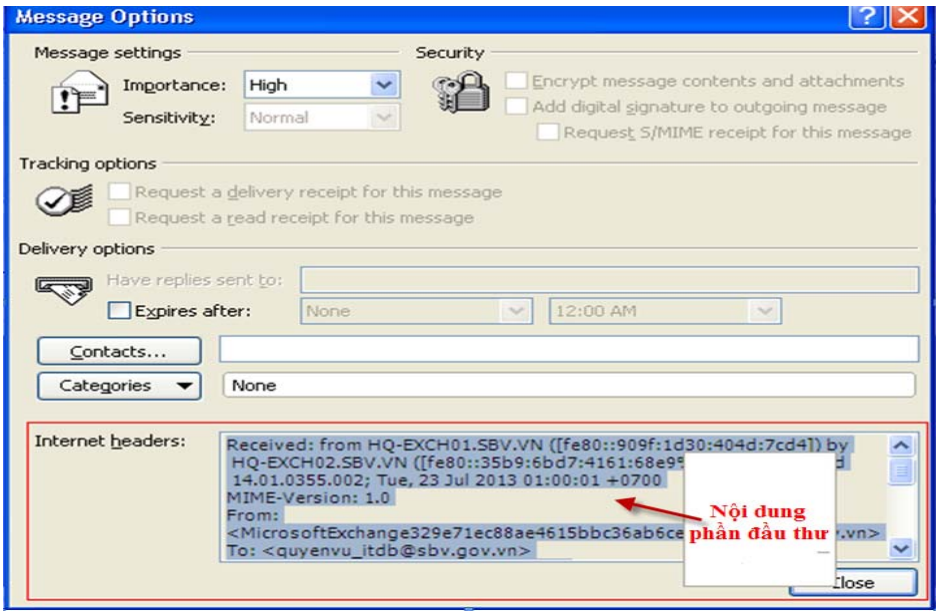
Chú ý: Nên copy Phần đầu thư vào tệp tin Notepad/Wordpad/Word để xem và tìm kiếm các trường thông tin một cách dễ dàng và nhanh chóng.

3.1. Đối với Microsoft Outlook 2007 và các phiên bản mới hơn.

- Nhấp **đúp chuột** vào thư điện tử cần xem Phần đầu thư, cửa sổ thư điện tử xuất hiện. Nhấp chọn **Options** như hình vẽ:



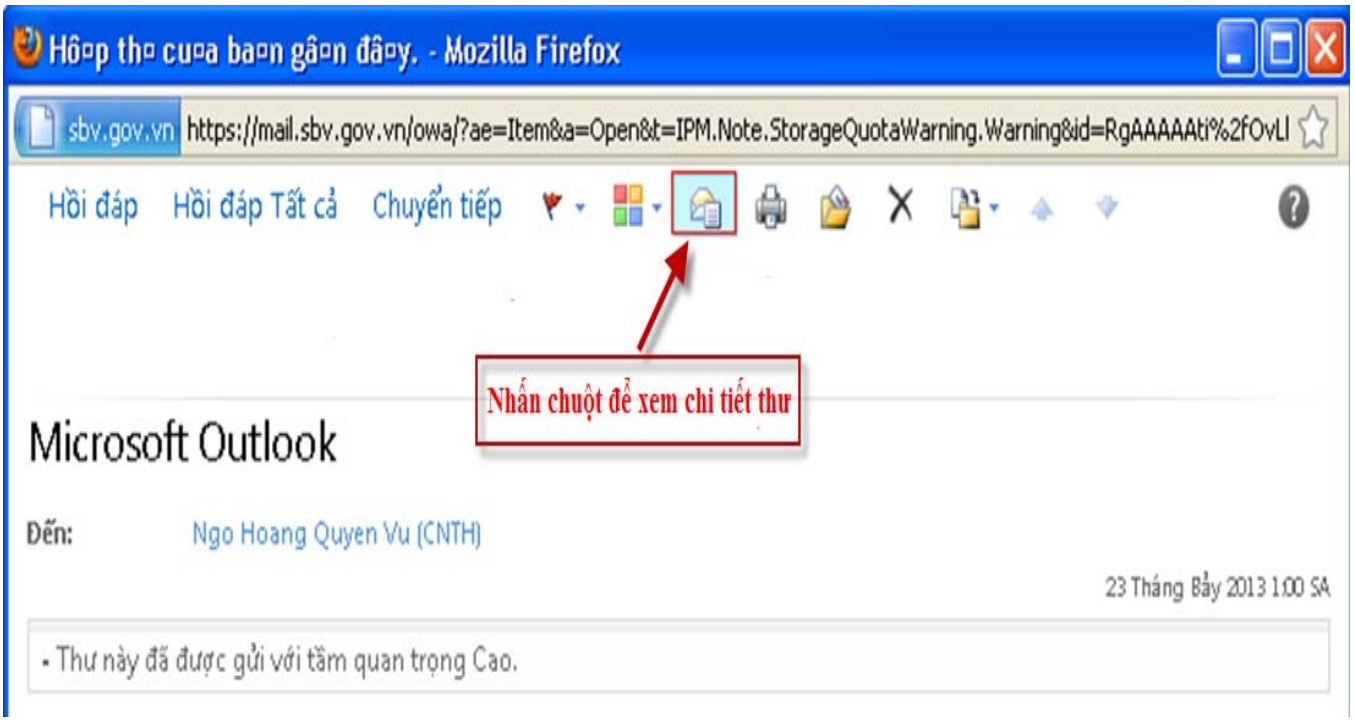
- Cửa sổ **Message Options** xuất hiện, giá trị mục **Internet Headers** là nội dung Phần đầu thư.



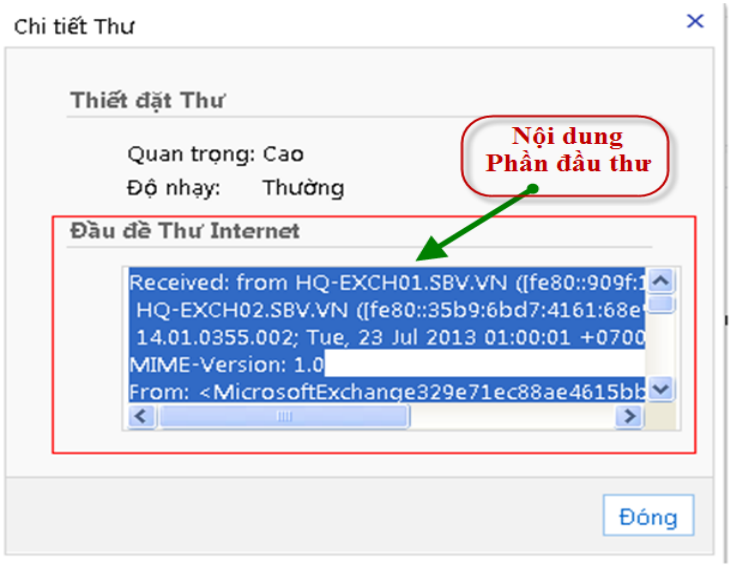
3.2. Đối với webmail của SBV.

3.2.1. Mail MS Exchange.

- Nhấp **đúp chuột** vào thư điện tử cần xem Phần đầu thư, cửa sổ thư điện tử xuất hiện. Nhấp chọn như hình dưới:

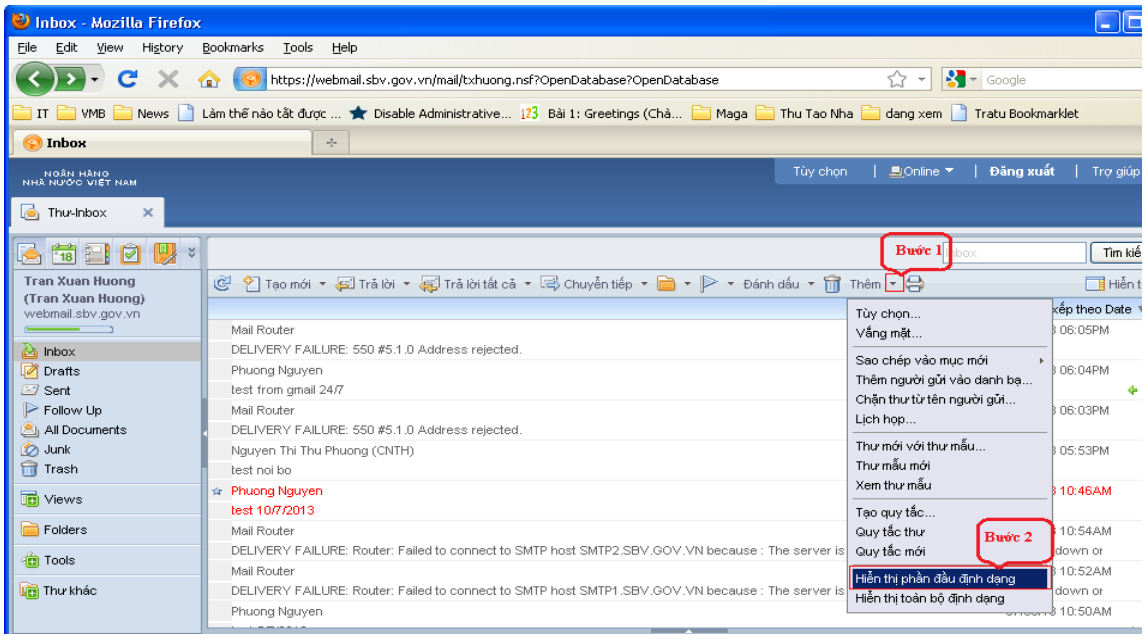


- Cửa sổ **Chi Tiết Thư** xuất hiện, giá trị mục **Đầu đề Thư Internet** là nội dung Phần đầu thư.



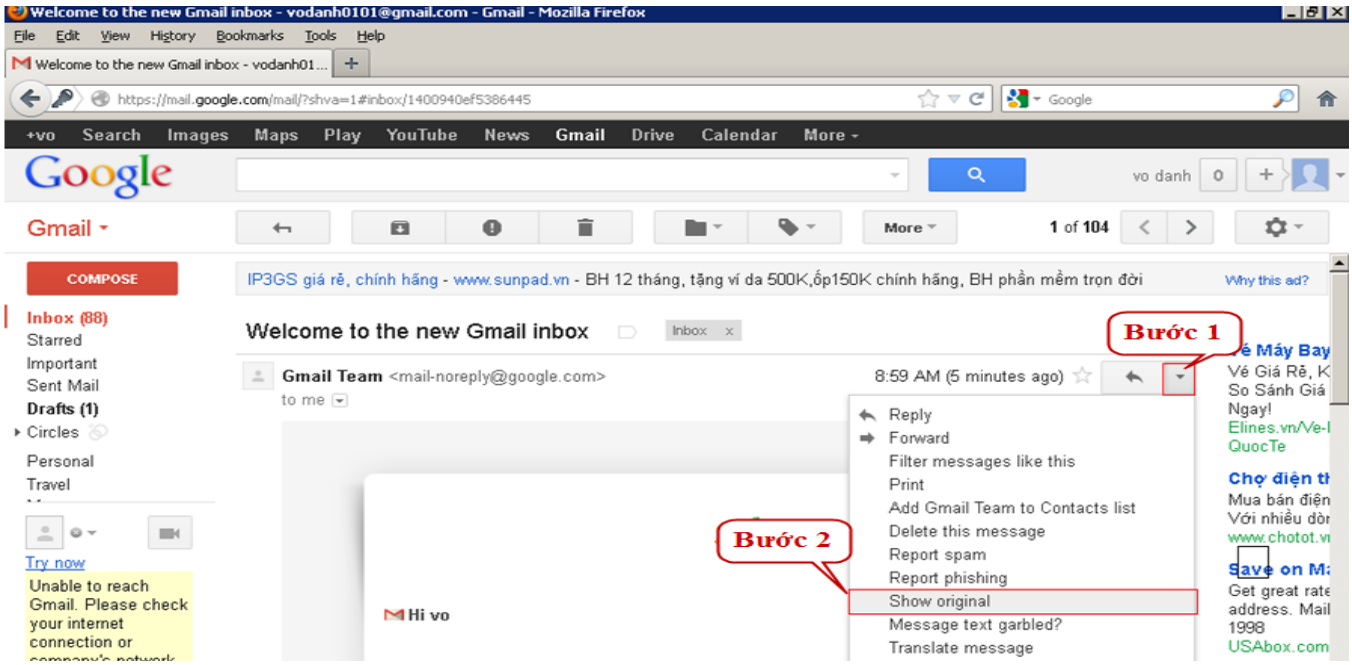
3.2.2. Mail Domino.

- Nhấp chọn thư cần xem phần đầu thư, nhấp chọn **Thêm -> Hiển thị phần đầu định dạng** như hình dưới. Cửa sổ nội dung Phần đầu thư sẽ xuất hiện.



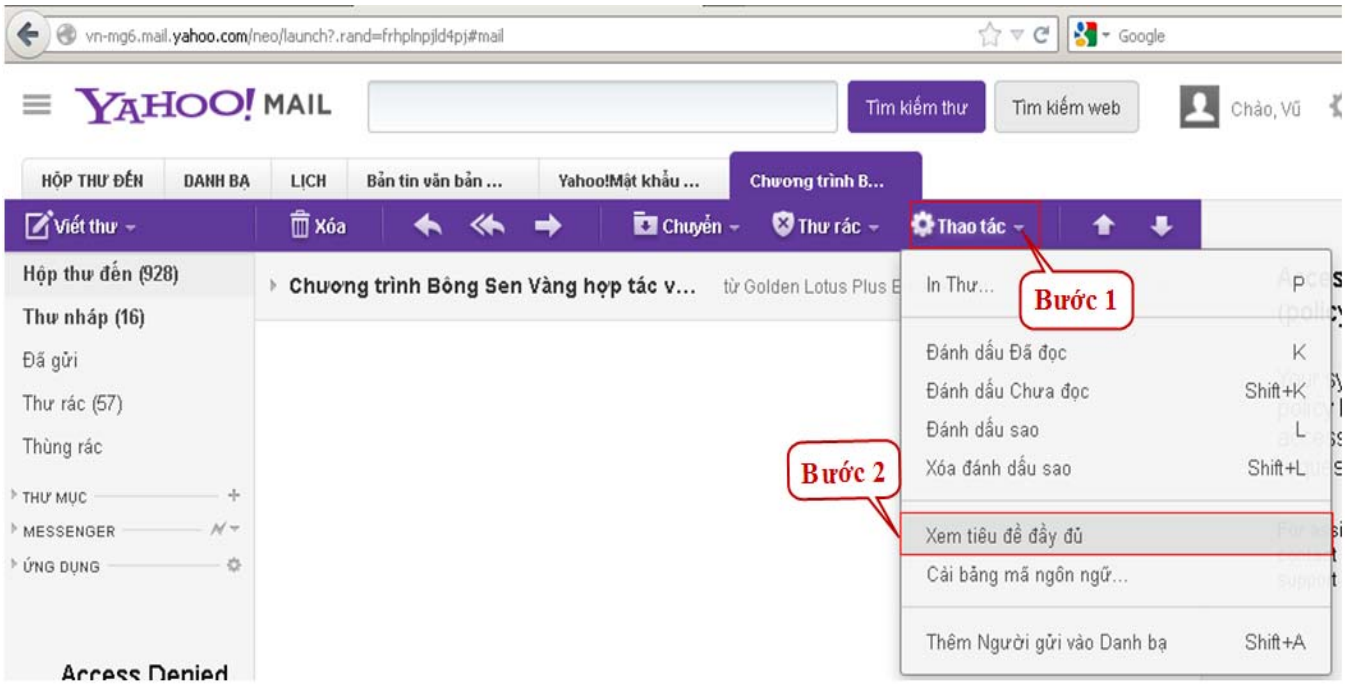
3.3. Đối với Gmail.

- Nhấp **đúp chuột** vào thư điện tử cần xem Phần đầu thư, nhấp chọn **Hiển thị thư gốc** hoặc **Show Original** như hình dưới. Cửa sổ nội dung Phần đầu thư sẽ xuất hiện.



3.4. Đối với Yahoo.

Nhấp chọn thư điện tử cần xem Phần đầu thư, nhấp chọn **Thao tác -> Xem tiêu đề đầy đủ** như hình dưới. Cửa sổ nội dung Phần đầu thư sẽ xuất hiện.



4. Báo cáo khi nhận được thư điện tử giả mạo.

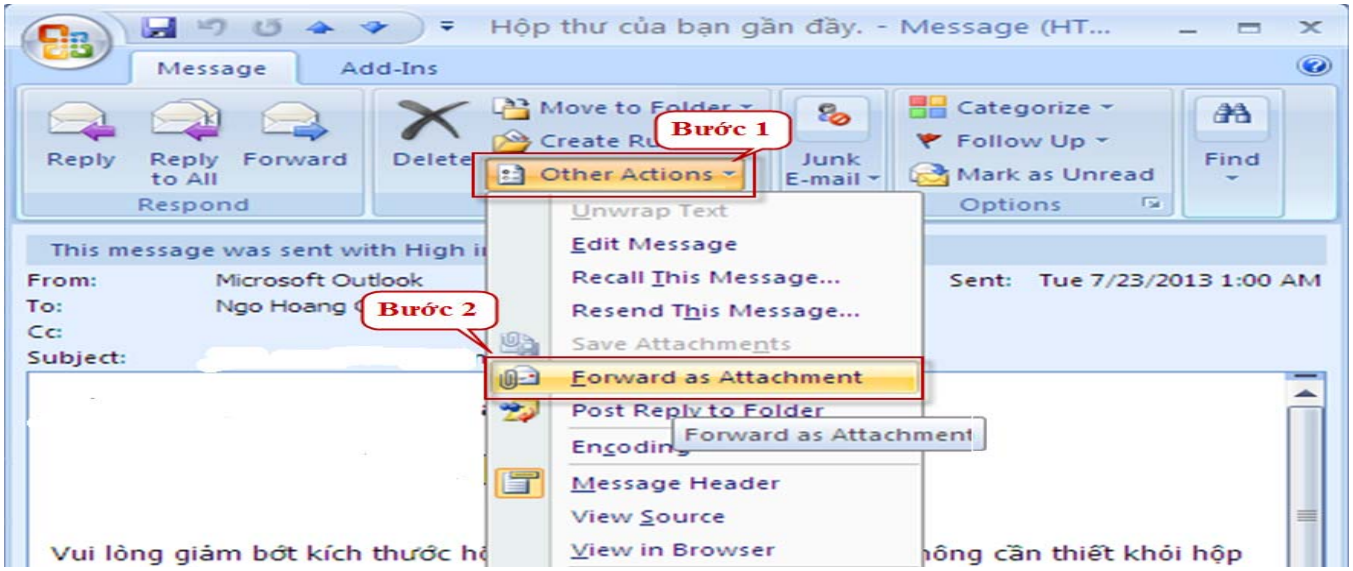
- Khi nhận được thư giả mạo (hoặc nghi ngờ giả mạo), đề nghị người nhận **gửi thư giả mạo dưới dạng tệp tin đính kèm** tới *itdb_service@sbv.gov.vn* (**Bộ phận HelpDesk của Cục CNTH**) theo mẫu sau:

> **Tiêu đề thư**: Báo cáo thư giả mạo
>
> **Nội dung thư**:
>
> Báo cáo thư giả mạo.
>
> - Tên người gửi: *Nguyễn Văn A*
> - *Đơn vị: ……*
> - Số điện thoại liên hệ: *09xxxxxx*

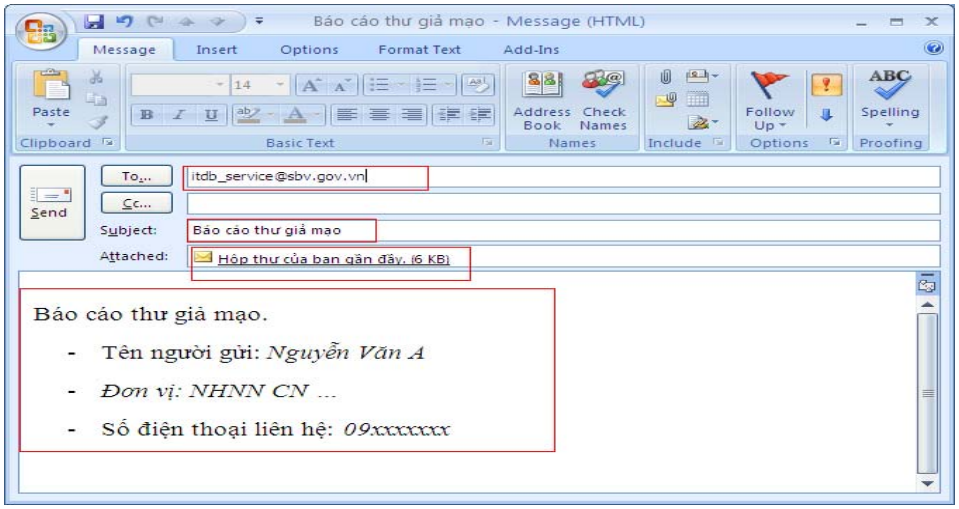
- Bộ phận trực HelpDesk của Cục CNTH khi nhận được thư này đề nghị chuyển tiếp cho Bộ phận HelpDesk của Phòng CA để Bộ phận an ninh bảo mật của Phòng CA xem xét, đánh giá và chuyển tiếp tới VNCERT - Trung tâm ứng cứu khẩn cấp máy tính Việt Nam theo địa chỉ *antoanthudientu@report.vncert.vn*, đồng thời gửi kết quả đánh giá thư lại cho Bộ phận HelpDesk. Bộ phận Helpdesk sẽ chuyển tiếp kết quả này cho người nhận thư giả mạo.

4.1. Đối với Microsoft Outlook 2007 và các phiên bản mới hơn.

- Nhấp **đúp chuột** thư cần gửi dưới dạng đính kèm, cửa sổ thư điện tử xuất hiện. Nhấp chọn **Other Actions -> Forward as Attachment** như hình dưới:



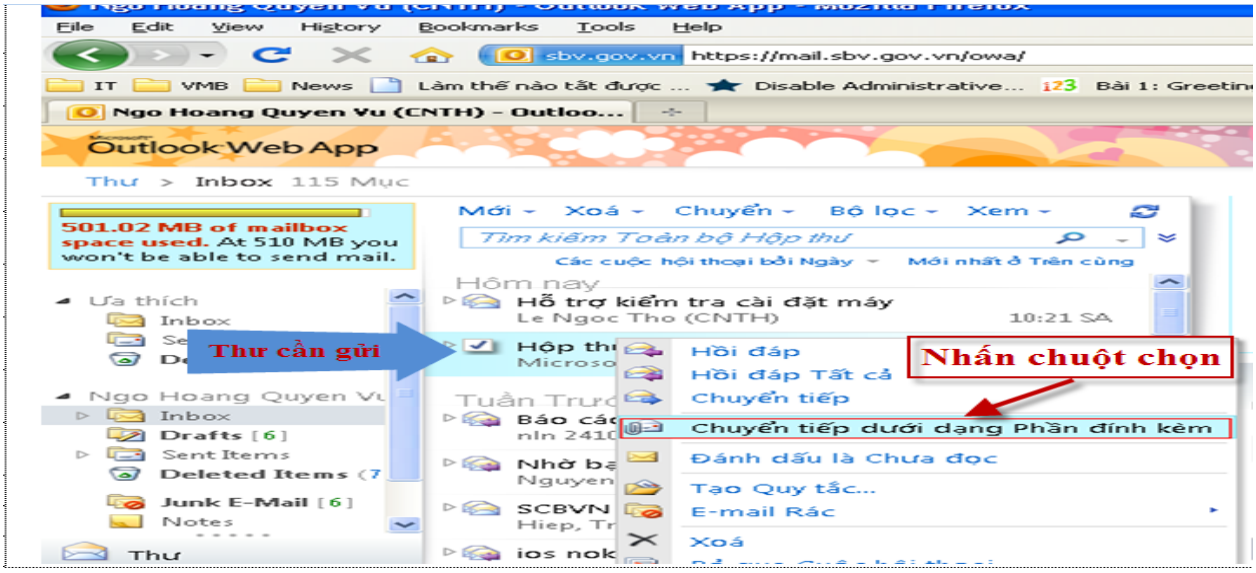
- Cửa sổ gửi thư dưới dạng đính kèm xuất hiện:



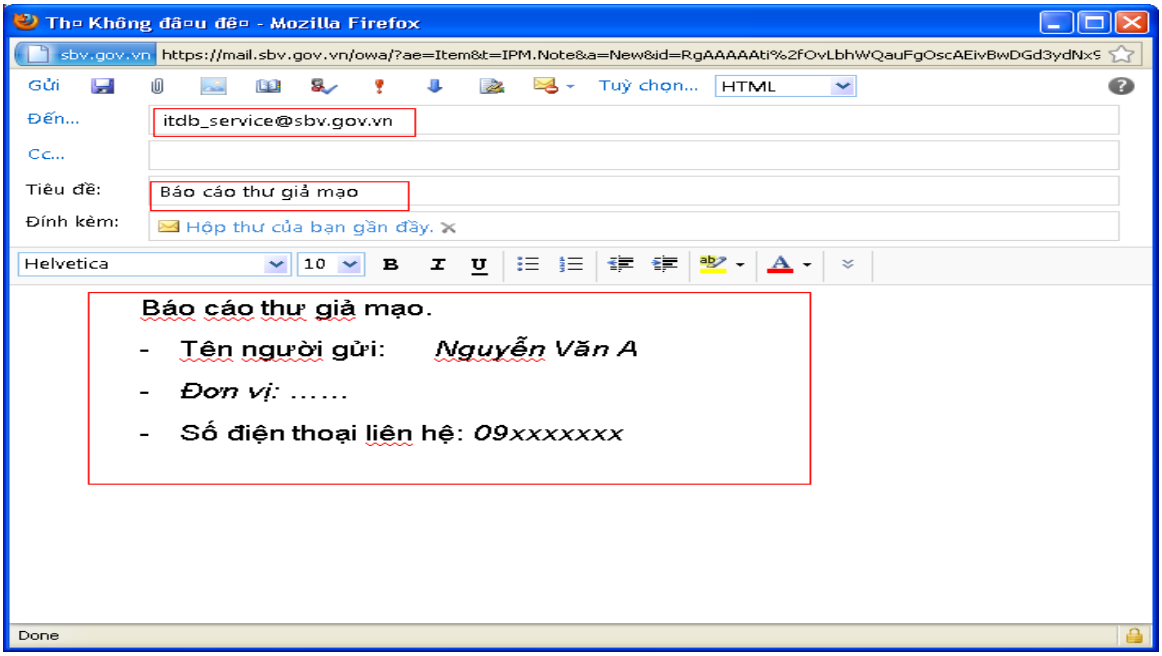
4.2. Đối với webmail của SBV.

4.2.1. Mail MS Exchange:

- Nhấp chuột phải vào thư cần gửi dưới dạng đính kèm, nhập chọn **Chuyển tiếp dưới dạng Phần đính kèm** như hình dưới:



- Cửa sổ gửi thư dưới dạng đính kèm xuất hiện:



4.2.2. Mail Domino:

Thực hiện lấy phần đầu thư như mục **3.2.2** sau đó copy nội dung phần đầu thư ra tập tin Notepad/Wordpad/Word, rồi gửi đính kèm theo thư điện tử theo mẫu ở trên.

4.3. Đối với Gmail và Yahoo.

Thực hiện lấy phần đầu thư như mục **3.3** và **3.4** sau đó copy nội dung phần đầu thư ra tập tin Notepad/Wordpad/Word, rồi gửi đính kèm theo thư điện tử theo mẫu ở trên.