NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC
Số: 603 /CNTH8
V/v: phòng chống mã độc WannaCry

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Hà Nội, ngày 15 tháng 05 năm 2017

KHẨN

Kính gửi: Các đơn vị trực thuộc Ngân hàng Nhà nước

Hiện nay mã độc WannaCry đang lây lan khắp các hệ thống mạng trên thế giới. Để đảm bảo an toàn cho hệ thống công nghệ thông tin (CNTT) của Ngân hàng Nhà nước, Cục CNTT đề nghị các đơn vị tổ chức thực hiện gấp các công việc sau:

1. Rà soát, cập nhật ngay bản vá lỗ hổng bảo mật MS17-010 cho các máy tính sử dụng hệ điều hành Windows. Đối với các máy được thiết lập domain Ngân hàng nhà nước sẽ được cập nhật tự động từ máy chủ Cục CNTT. Đối với các máy tính chưa thiết lập domain Ngân hàng Nhà nước hoặc máy tính khác tham khảo hướng dẫn cập nhật trực tiếp từ mạng Internet theo hướng dẫn: https://support.microsoft.com/en-us/help/3067639/how-to-get-an-update-through-windows-update

2. Kiểm tra việc cập nhật phiên bản mới nhất của phần mềm phòng chống mã độc hại cài đặt trên hệ thống máy tính của đơn vị.

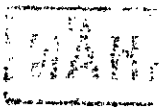
3. Tắt các dịch vụ SMB (Server Message Block) trên máy chủ, máy trạm (nếu không sử dụng) theo hướng dẫn tại https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

4. Đối với các đơn vị có hệ thống CNTT riêng không do Cục CNTT quản trị (CIC, Thời báo Ngân hàng, Học viện Ngân hàng,...), đề nghị thực hiện:

- Theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc WannaCry và cập nhật vào các hệ thống an ninh mạng (Firewall, IDS/IPS,...) các thông tin nhận dạng tại Phụ lục đính kèm.
- Rà soát việc phân vùng mạng LAN và thiết lập hạn chế kết nối qua các cổng của dịch vụ SMB là: 445, 137, 138, 139.

5. Phổ biến cho cán bộ các biện pháp phòng ngừa mã độc

- Không tải về và mở các tệp tin không rõ nguồn gốc từ Internet như: Các tệp tin đính kèm gửi qua thư điện tử; các đường dẫn gửi qua các công cụ nhắn tin, các tệp tin chia sẻ trên mạng xã hội.



- Cảnh giác trước các thư điện tử giả mạo người thân có đính kèm tệp tin hoặc đường dẫn lừa đảo. Tham khảo hướng dẫn phát hiện thư giả mạo đính kèm công văn 744/CNTH8 ngày 25/7/2013 của Cục CNTT.

6. Kịp thời thông báo ngay cho Cục CNTT khi phát hiện các sự cố, mối đe dọa liên quan đến mã độc WannaCry để phối hợp xử lý.

Thông tin liên hệ: Phòng An ninh thông tin - Cục CNTT; 64 Nguyễn Chí Thanh - Đống Đa - Hà Nội; Điện thoại: 04.32595983 hoặc 0123.8595983; Fax: 04.38358135; Email: antt@sbv.gov.vn; Hoặc bộ phận hỗ trợ kỹ thuật Cục CNTT: điện thoại 04.32595986 hoặc 04.37756789-ext: 8888; Email: hotrotinhoc@sbv.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- PTĐ Nguyễn Kim Anh (để b/c);
- Bộ phận Helpdesk (để phối hợp);
- Lưu: CNTH, CNTH8.

Đính kèm:
- 744/CNTH8;
- Phụ lục.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC
NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

Lê Mạnh Hùng

PHỤ LỤC: THÔNG TIN VỀ MÃ ĐỘC WANNACRY

I. Danh sách các máy chủ điều khiển mã độc (C&C Server)

STT	Địa chỉ IP C&C	STT	Địa chỉ IP C&C
1	128.31.0.39	18	213.239.216.222
2	136.243.176.148	19	213.61.66.116
3	146.0.32.144	20	38.229.72.16
4	163.172.153.12	21	50.7.151.47
5	163.172.185.132	22	50.7.161.218
6	163.172.25.118	23	51.255.41.65
7	171.25.193.9	24	62.138.10.60
8	178.254.44.135	25	62.138.7.231
9	178.254.44.135	26	79.172.193.32
10	178.62.173.203	27	81.30.158.223
11	185.97.32.18	28	82.94.251.227
12	188.138.33.220	29	83.162.202.182
13	188.166.23.127	30	83.169.6.12
14	192.42.115.102	31	86.59.21.38
15	193.23.244.244	32	89.45.235.21
16	198.199.64.217	33	94.23.173.93
17	212.47.232.237		

II. Danh sách tên tập tin

STT	File name	STT	File Name
1	@WanaDecryptor@.exe	6	taskse.exe
2	b.wnry	7	t.wnry
3	c.wnry	8	u.wnry
4	s.wnry	9	Các file với phần mở rộng ".wnry"
5	taskdl.exe	10	Các file với phần mở rộng ".WNCRY"

III. Danh sách mã băm (Hash SHA-256)

STT	SHA-256
1	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

2	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
3	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
4	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
5	428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
6	5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
7	62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
8	72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
9	85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
10	a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
11	a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
12	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
13	eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
14	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
15	2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
16	7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
17	a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
18	fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
19	9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
20	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
21	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
22	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

NGÂN HÀNG NHÀ NƯỚC
VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC

Số: 744 /CNTH8
V/v Hướng dẫn
phát hiện thư điện tử giả mạo

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 25 tháng 7 năm 2013

Kính gửi:
- Các Vụ, Cục, Đơn vị trực thuộc Ngân hàng Nhà nước;
- Các NHNN chi nhánh tỉnh, thành phố.

Theo thông báo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), gần đây xuất hiện các trường hợp phát tán thư điện tử mạo danh cơ quan nhà nước, cá nhân có uy tín nhằm tung các thông tin có nội dung sai trái, một số thư giả mạo còn chứa mã độc ẩn trong các tệp tin đính kèm dưới dạng pdf, doc, exe, gây mất an toàn thông tin nếu người nhận thư vô tình mở các tệp tin này. Để phát hiện thư điện tử giả mạo, Cục Công nghệ tin học (CNTH) đề nghị Quý Đơn vị phổ biến, hướng dẫn cho người sử dụng thư điện tử thực hiện theo tài liệu "Hướng dẫn phát hiện thư giả mạo". Tài liệu "Hướng dẫn phát hiện thư giả mạo" được đăng tại Website NHNN http://sbv.gov.vn, chuyên mục: *Các hoạt động khác của NHTW -> Công nghệ thông tin – Truyền thông -> Hỗ trợ kỹ thuật.*

Trong quá trình thực hiện, nếu có vướng mắc đề nghị Quý Đơn vị liên hệ Bộ phận hỗ trợ kỹ thuật - Cục CNTH theo số điện thoại 04.32595986, IP Phone 04.8888 hoặc thư điện tử itdb_service@sbv.gov.vn để được hướng dẫn.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Chi Cục để thực hiện;
- Các phòng ban để thực hiện;
- Lưu CNTH8, CNTH.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ TIN HỌC
NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

Lê Mạnh Hùng

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/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

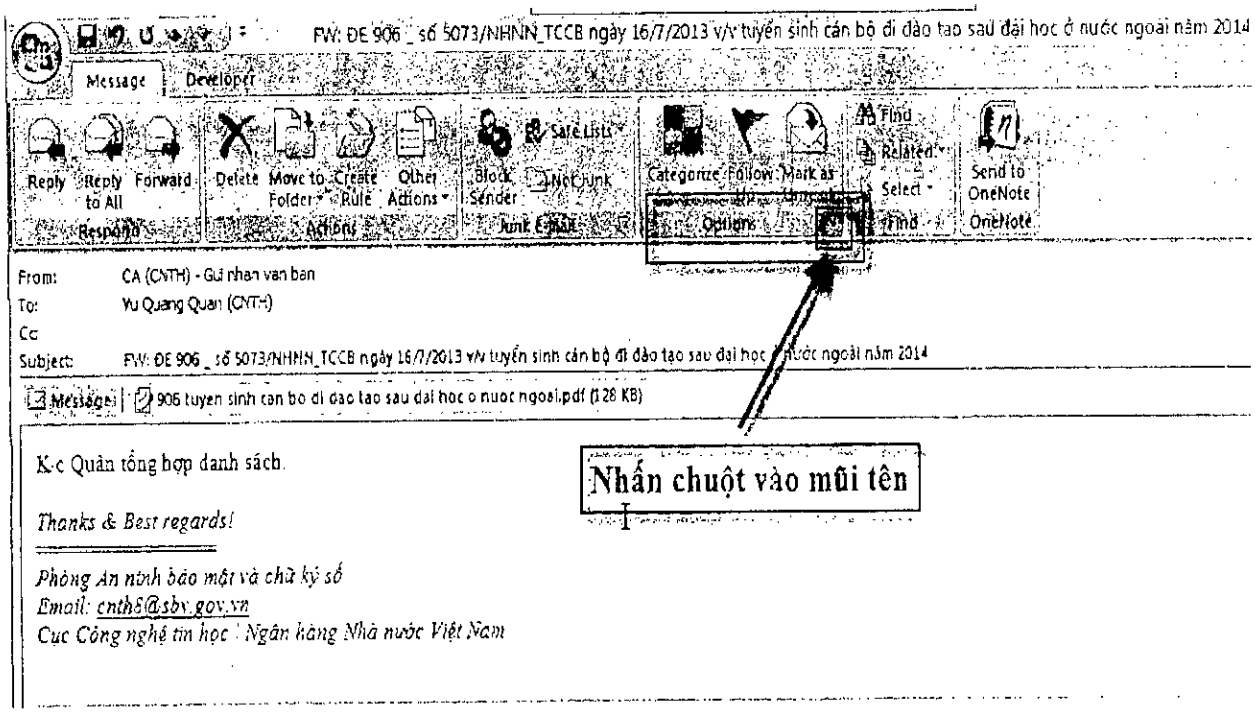
Subject: Em ơi password thẻ ATM Đông Á, Em mới đổi là gì nhỉ?

3. HƯỚNG DẪN XEM PHẦN ĐẦU THƯ CỦA MỘT THƯ ĐIỆN TỬ.

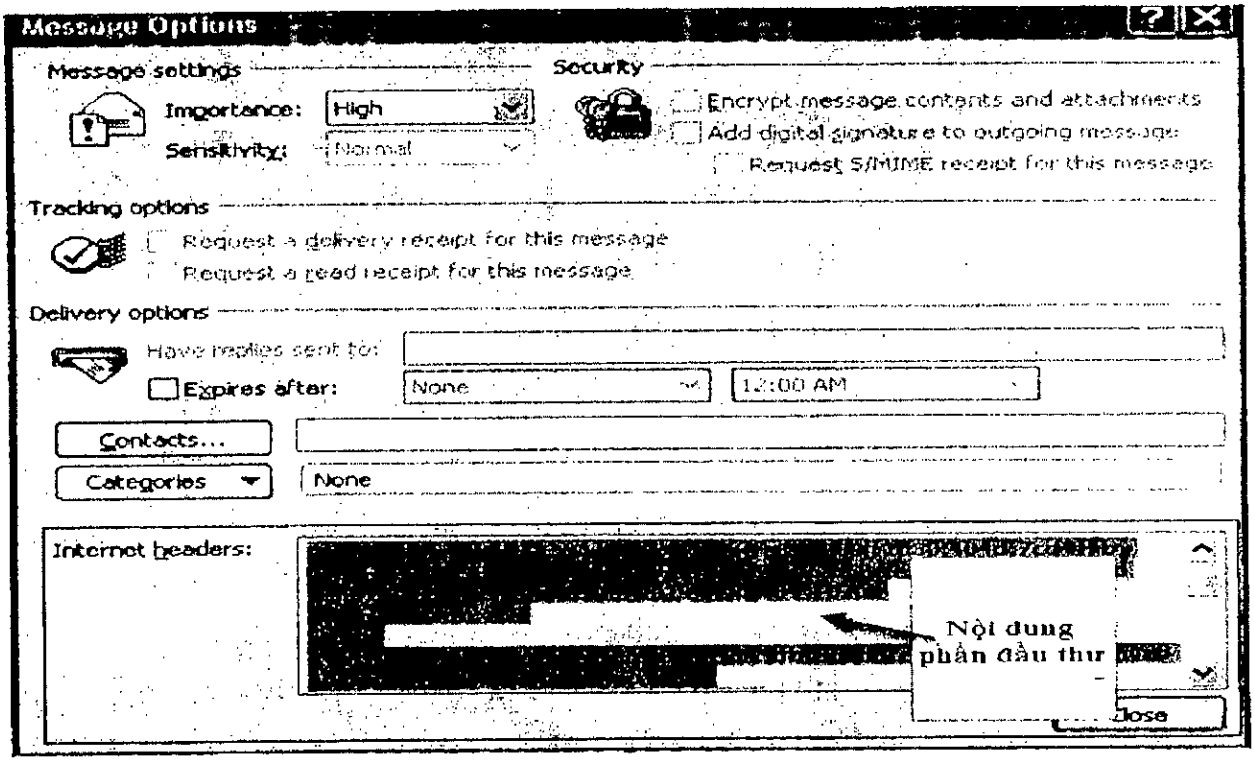
Chú ý: Nên copy Phần đầu thư vào tệp tin Notepad/Wordpad/Word để xem và tìm kiếm các trường thông tin một cách dễ dàng và nhanh chóng.

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:

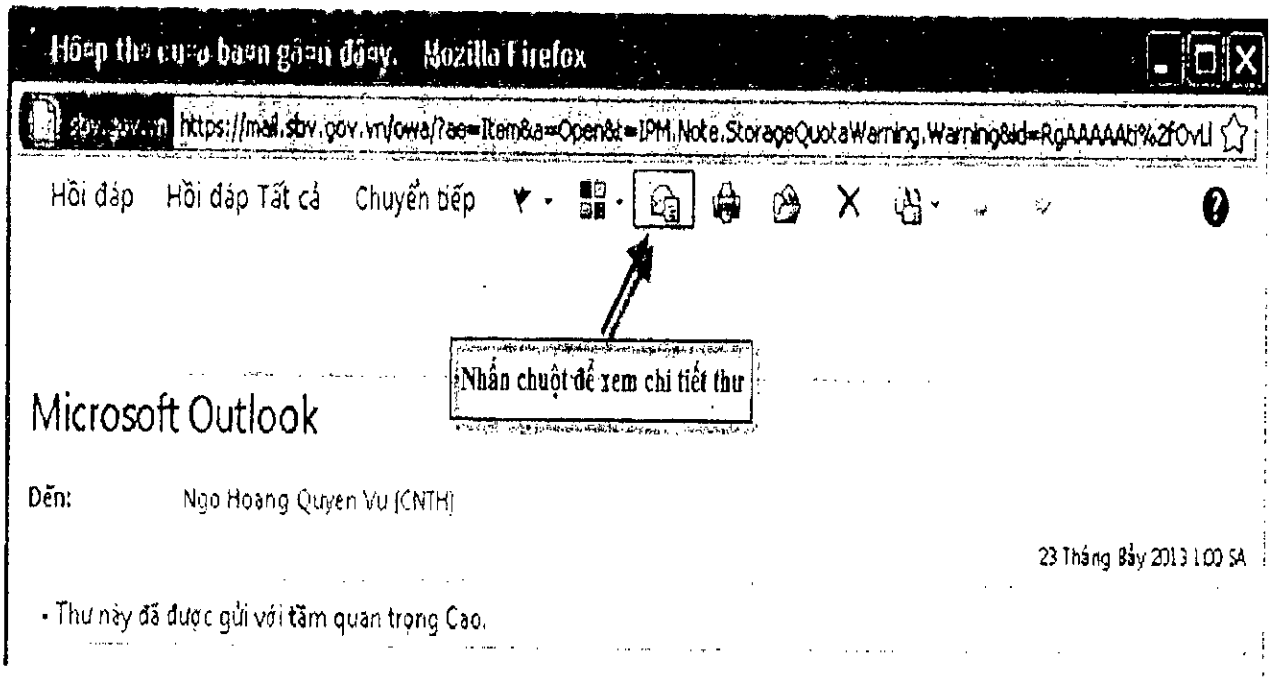


- Cửa sổ **Message Options** xuất hiện, giá trị mục **Internet Headers** là nội dung Phần đầu thư.

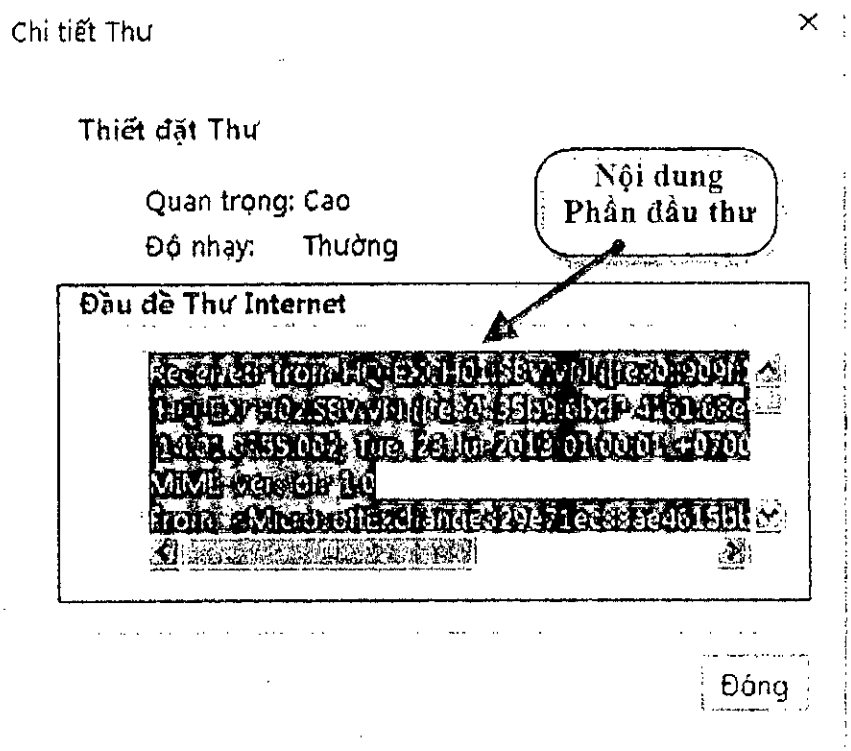


3.2. Đối với webmail của SBV

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

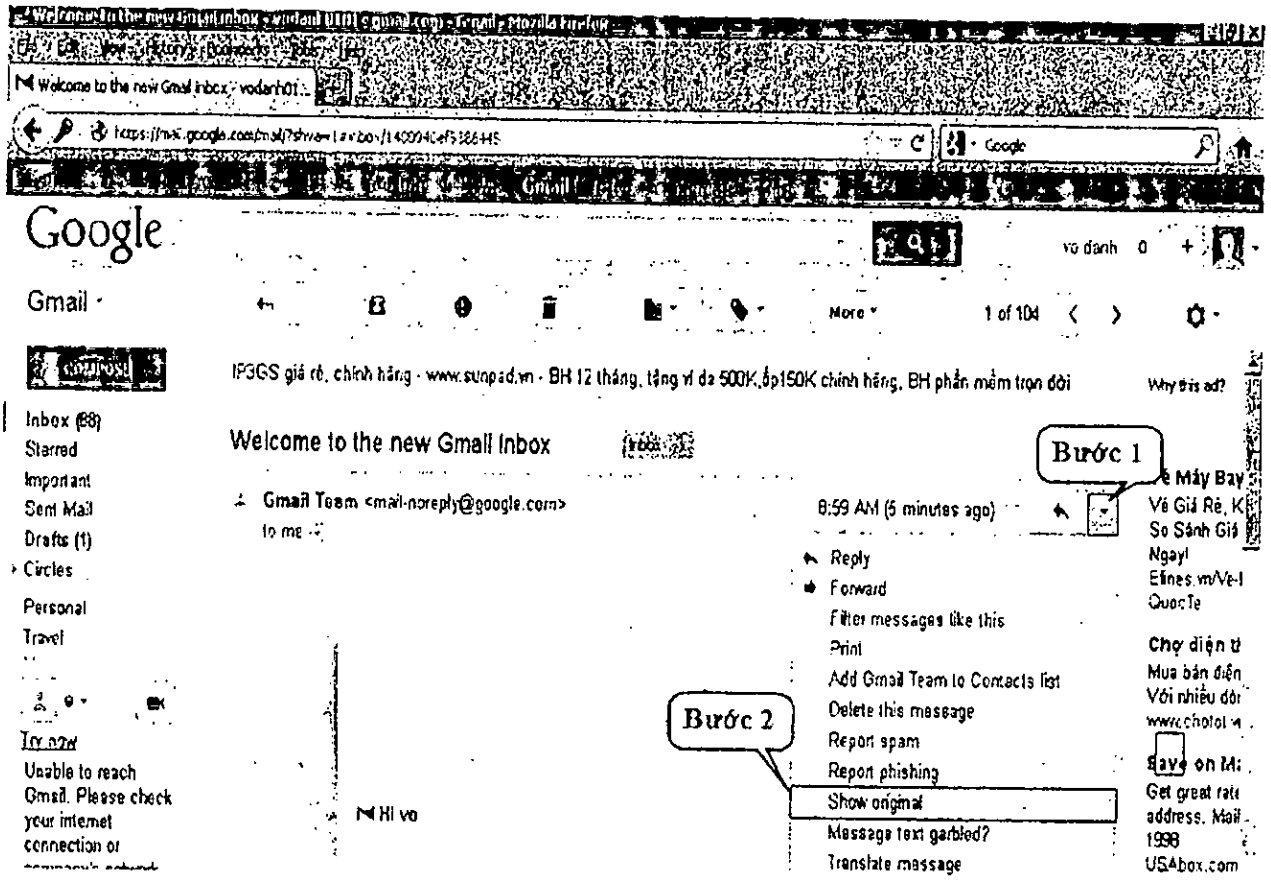


- Cửa sổ **Chi Tiết Thư** xuất hiện, giá trị mục **Đầu đề Thư Internet** là nội dung Phần đầu thư. Chú ý nên copy nội dung này vào tệp Notepad/Wordpad/Word để xem và tìm kiếm các trường thông tin cho dễ và nhanh.



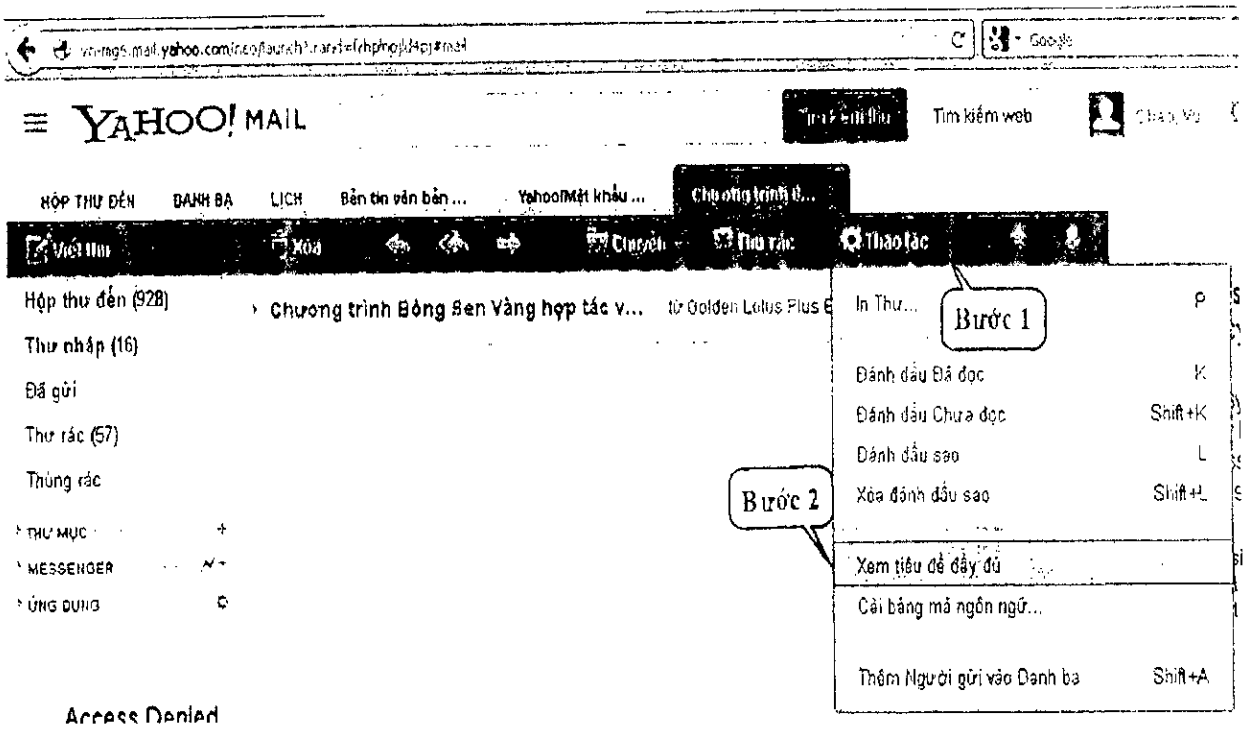
3.3. Đối với Gmail.

- 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 và theo mẫu sau:

Tiêu đề thư: Báo cáo thư giả mạo

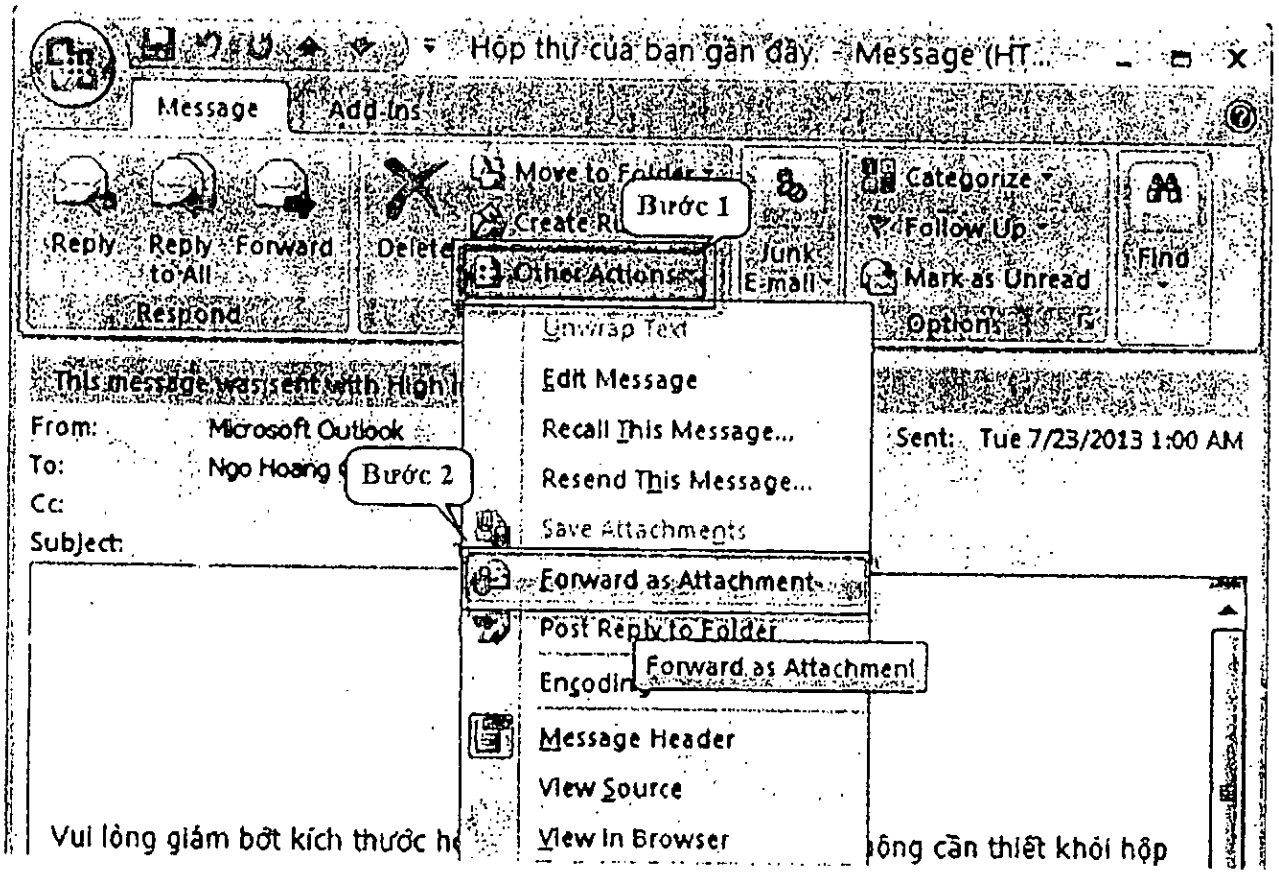
Nội dung thư:

Báo cáo thư giả mạo.

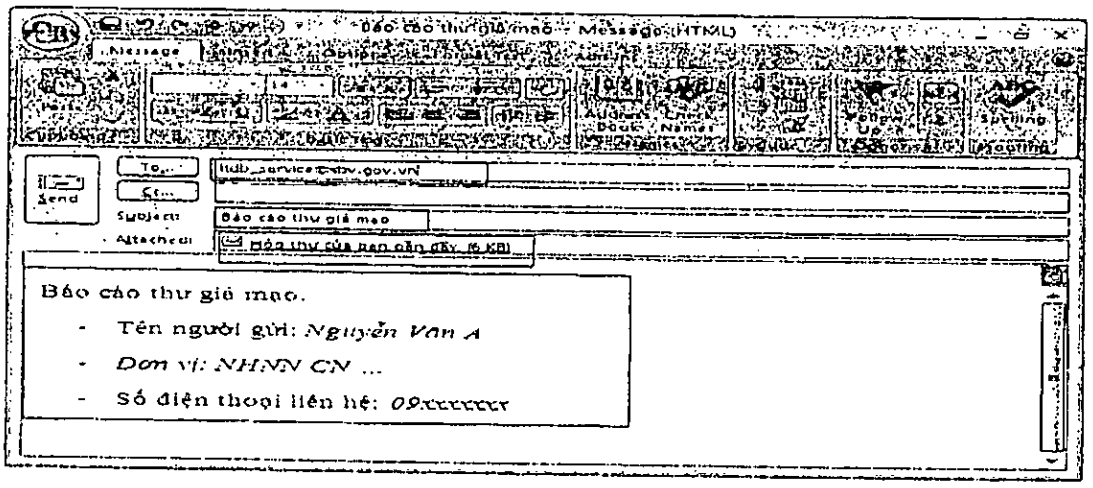
- Tên người gửi: *Nguyễn Văn A*
- *Đơn vị: .....*
- Số điện thoại liên hệ: *09xxxxxxx*

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:

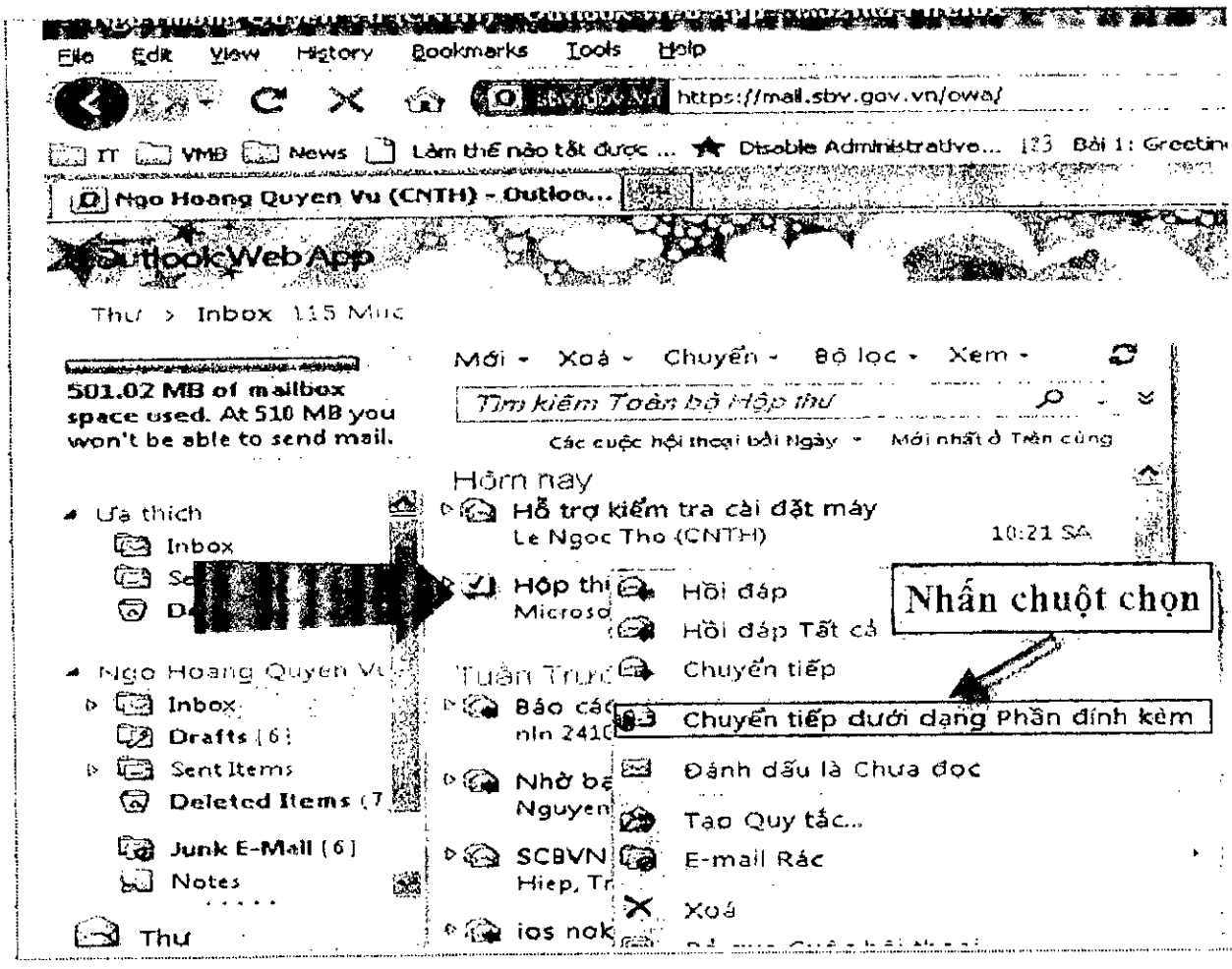


- Cửa sổ gửi thư dưới dạng đính kèm xuất hiện:

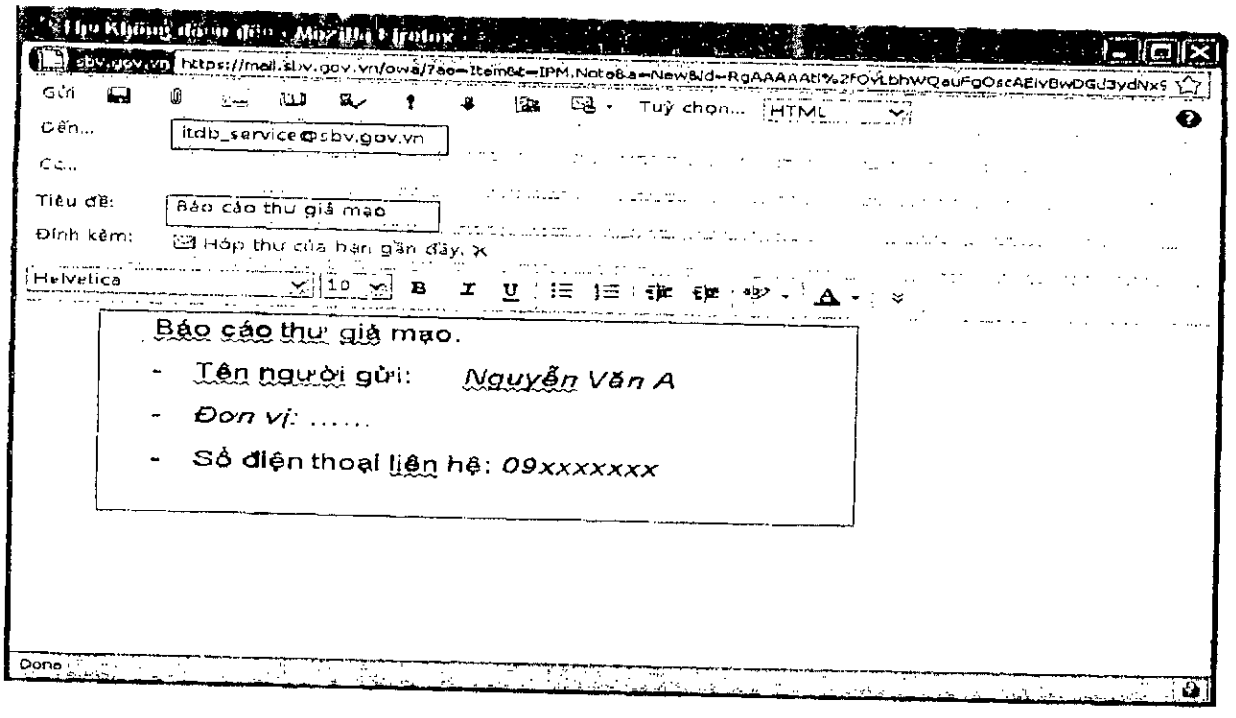


4.2. Đối với webmail của SBV.

- Nhập 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:



4.3. 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.