## 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 Đ	ÍCH:	3
II.	NỘI DƯ	NG HƯỚNG DẪN:	3
1.	Định dạ	ng của một thư điện tử	3
2.	Phương	pháp phát hiện thư điện tử giả mạo	4
3.	Hướng	dẫn xem Phần đầu thư của một thư điện	5
3	.1. Đối v	với Microsoft Outlook 2007 và các phiên bản mới hơn	6
3	.2. Đối v	với webmail của SBV	7
	3.2.1.	Mail MS Exchange	7
	3.2.2.	Mail Domino	8
3	.3. Đối v	với Gmail	8
3	.4. Đối v	với Yahoo	9
4.	Báo cáo	khi nhận được thư điện tử giả mạo	9
4	.1. Đối v	với Microsoft Outlook 2007 và các phiên bản mới hơn	10
4	.2. Đối v	với webmail của SBV	11
	4.2.1.	Mail MS Exchange:	11
	4.2.2.	Mail Domino:	11
4	.3. Đối v	với Gmail và Yahoo	



## 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 này chủ thư điện tử này.

## 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 <u>http://whois.domaintools.com</u> 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 <u>http://whois.domaintools.com</u> 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: <u>BiGiaMao@sbv.gov.vn</u>

Reply-To: BiGiaMao@sbv.gov.vn

To: <u>BiLua@sbv.gov.vn</u>

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

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

<u>Chú ý:</u> 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.

ITDB



## 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:

Message De	♥ ▼ FW: ÐE 906 _ số 5 eveloper	073/NHNN_TCCB ngày 1	.6/7/2013 v/v tuyển sinh cá	n bộ đi đào tạ	o sau đại học ở nư	ớc ngoài năm 2014
Reply Reply Forward to All Respond	Delete Move to Create Other Folder * Rule Actions * Actions	Block Sender Junk E-mail	Categorize Follow Mark as Up Unread Options	A Find → Related + Select + Find	Send to OneNote OneNote	
From:         CA (CNTH) -           To:         Vu Quang Qu           Cc:         Subject:           FW: DE 906         전 005 thm	Gui nhan van ban Jan (CNTH) _ sõ 5073/NHNN_TCCB ngày 16/7/201	3 v/v tuyển sinh cán bộ đi đ	ào tạo sau đại học ở nước ngo			
K/c Quân tổng hợp đ Thanks & Best regar	lanh sách. <i>'ds!</i>	Nhá	n chuột vào mũ	ii tên		
Phòng An ninh bảo r Email: <u>cnth8@sbv.g</u> Cục Công nghệ tin h	= mật và chữ ký số <u>ov.vn</u> nọc   Ngân hàng Nhà nước Việ	t Nam				

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

Message Options		? 🛛
Message settings	Security	
Importance: Sensitivity:	High   High  Normal  Request S/MIN	contents and attachments ire to outgoing message 4E receipt for this message
Request a de     Request a re     Req     Request a re     Request a re     Request a re     Request a	livery receipt for this message ad receipt for this message t to: None	
Categories V N	one ceived: from HQ-EXCH01.SBV.VN ([fe80::909f:1d Q-EXCH02.SBV.VN ([fe80::35b9:6bd7:4161:68e99 4.01.0355.002; Tue, 23 Jul 2013 01:00:01 +0700 IME-Version: 1.0 om: MicrosoftExchange329e71ec88ae4615bbc36ab6ce c: <quyenvu_itdb@sbv.gov.vn></quyenvu_itdb@sbv.gov.vn>	30:404d:7cd41) by Nội dung phần đầu thư lose

Hướng dẫn phát hiện thư điện tử giả mạo



#### 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.



Hướng dẫn phát hiện thư điện tử giả mạo





#### 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.

😢 Inbox - Mozilla Firefox								
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory	Bookmarks Tools Help							
C ×	https://webmail.sbv.gov.vn/mail/txhuong.nsf?OpenDatabase?OpenDatabase	☆ - Google						
🚞 IT 🚞 VMB 🚞 News 📄	Làm thế nào tắt được 🚖 Disable Administrative 123 Bài 1: Greetings (Chà 🚞 Maga 🚞 Thu Tao Nh	na 🚞 dang xem 📄 Tratu Bookm	arklet					
📀 Inbox	*							
NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	Tùy chọi	n 📔 📃 Online 🔻 📔 Đăng xuấ	<b>ắt  </b> Trợ giúp					
💽 Thu-Inbox 🗙								
🍝 🗃 🔜 🗹 🛄 ×		Bước 1	Tîm kiế					
Tran Xuan Huong	🎯 Y Tạo mới 🔹 🚑 Trả lời 🔹 🚚 Trả lời tất cả 🔹 🖃 Chuyển tiếp 🔹 📄 👻 Þ 🔹 Đánh dấu 👻 🍿	Thêm 💽 🔒	📑 Hiễn t					
(Tran Xuan Huong) webmail.sby.gov.yn		Tùy chon	xếp theo Date					
	Mail Router	Vắng mặt	8 06:05PM					
실 Inbox	DELIVERY FAILURE: 550 #5.1.0 Address rejected.							
📝 Drafts	Phuong Nguyen	Thêm người gửi vào danh ha	3 06:04PM					
🖅 Sent	test from gmail 24/7	Chăn thự từ tên người gửi	4					
Follow Up	Mail Router	Lich hop	3 06:03PM					
All Documents	DELIVERY FAILURE: 550 #5.1.0 Address rejected.	Thu a mái cuái thu a mắc c						
😥 Junk	Nguyen Thi Thu Phuong (CNTH)	Thur mor vor internau	8 05:53PM					
m Irasn	test noi bo	Xem thự mẫu						
🛅 Views	er Phuong Nguyen	4	9 10:46AM					
Eolders	Mail Router	Duy tắc thự	10:54AM					
	DELIVERY FAILURE: Router: Failed to connect to SMTP host SMTP2.SBV.GOV.VN because : The server is	Quy tắc mới	down or					
Tools	Mail Router		B 10:52AM					
🛅 Thư khác	DELIVERY FAILURE: Router: Failed to connect to SMTP host SMTP1.SBV.GOV.VN because : The server is	Hiện thị phán dâu dịnh dạng Hiển thị toàn hộ định dạng	down or					
	Phuong Nguyen	nien mitoan so dinn dang	-8 10:50AM					

## 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 số 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 số nội dung Phần đầu thư sẽ xuất hiện.

• The second sec						☆ マ C Soogle		
≡ YAHOO!	MAIL			Tim	kiếm thư	Tîm kiếm web	L Chảo, Vũ	
HỘP THƯ ĐẾN DANH BẠ	LICH	Bản tin văn bản	Yahoo!Mật khẩu	Chwong trình B			_	
🗹 Viết thư 🗸	🗍 Xóa	* *	\Rightarrow 🚺 Chuyển	– 🛛 🕺 Thư rác –	🗘 Thao tác	- <b>*</b> +		
Hộp thư đến (928)	> Chươn	g trình Bông Ser	n Vàng hợp tác v	từ Golden Lotus Plus E	In Thư		Apce	
Thư nháp (16)						Buoc 1	(polie	
Đã gửi					Đánh dấu	Đã đọc	К	
Thư rác (57)					Đánh dấu	Chưa đọc	Shift+K	
Thùng rác				$\frown$	Đánh dấu	sao	L	
				Bước 2	Xóa đánh	dấu sao	Shift+L	
MESSENGER - MY				T	Xem tiêu	để đầy đủ	Fortes	
Ի ứng dụng Φ					Cải bảng	mã ngôn ngữ	t	
					Thêm Na	rời gửivào Dan hba	Shift+A	
Access Denied						3		

#### 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:





- 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:

🕲 The Khôn	g đâ¤u đê¤ - Mozilla Firefox						
sbv.gov.v	n https://mail.sbv.gov.vn/owa/?ae=Item&t=IPM.Note&a=New&id=RgAAAAAti%2fOvLbhWQauFgOscAEivBwDGd3ydNx5	☆					
Gửi 🔛	🌒 🔜 🛍 🎭 📍 🌡 🎯 🧏 - Tuỳ chọn HTML 🛛 🖌	?					
Đến	··· itdb_service@sbv.gov.vn						
Сс							
Tiêu đề:	Báo cáo thư giả mạo						
Ðính kèm:	🖂 Hộp thư của bạn gần đầy. 🗙						
Helvetica	✓ 10 ✓ B I U 注 注 详 详 学 ▲ · ×						
	Báo cáo thự giả mạo.						
· ·	- <u>Tên người</u> gửi: <u>Nguyễn</u> Văn A						
	- Đơn vị:						
	- Số điện thoại liện hệ: <i>09xxxxxx</i>						
Done							

#### 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.