VIỆN HÀN LÂM
KHOA HỌC VÀ CÔNG NGHỆ VN
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Số: 366 /THTT
V/v khuyến nghị một số biện pháp kỹ thuật để ngăn chặn thư điện tử giả mạo

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

Hà Nội, ngày 19 tháng 9 năm 2019

Kính gửi: Các đơn vị trực thuộc Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Trong thời gian vừa qua, tình hình mất an toàn thông tin trên mạng của các cơ quan Nhà nước và các tổ chức, cá nhân trong nước là rất nghiêm trọng. Trong đó, nổi cộm lên vấn đề sơ hở trong quản lý và sử dụng các hòm thư điện tử, tạo điều kiện cho tin tặc ăn cắp thông tin trên máy tính, phát tán virus và các tài liệu có nội dung không được kiểm chứng.

Gần đây, trong khoảng tháng 6-8/2019, Trung tâm Tin học và Tính toán đã phát hiện hình thức phát tán thư điện tử bằng cách mạo danh các cơ quan nhà nước, cá nhân có uy tín, nhằm phát tán các thông tin có nội dung sai trái. Một số thư điện tử giả mạo còn chứa mã độc ẩn trong các tệp tin đính kèm dưới dạng PDF, DOC/X, EXE… hoặc trên các trang web có chứa virus được liên kết gián tiếp thông qua đường dẫn trong thư điện tử. Để phát hiện thư điện tử giả mạo, người sử dụng có thể tham khảo một số biện pháp trong tài liệu hướng dẫn trong phần Phụ lục.

Khi phát hiện các thư điện tử giả mạo hoặc có chứa mã độc, kính đề nghị quý Cơ quan, người dùng làm theo hướng dẫn trong tài liệu để cảnh báo và ứng phó kịp thời.

Lưu ý, khi phổ biến thông tin cho người sử dụng hệ thống thư điện tử, Trung tâm Tin học và Tính toán chỉ gửi thông báo duy nhất bằng **01** địa chỉ là: **nguyenhoan@cic.vast.vn** hoặc sẽ gửi trực tiếp văn bản qua đường hành chính - văn thư.

Mọi chi tiết xin liên hệ Nguyễn Thị Hoan, Phó Trưởng phòng Công nghệ phần mềm - Trung tâm Tin học và Tính toán, điện thoại 0978822440, hòm thư điện tử: nguyenhoan@cic.vast.vn.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Lưu: VT, NTH50.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Ngô Văn Thanh

PHỤ LỤC

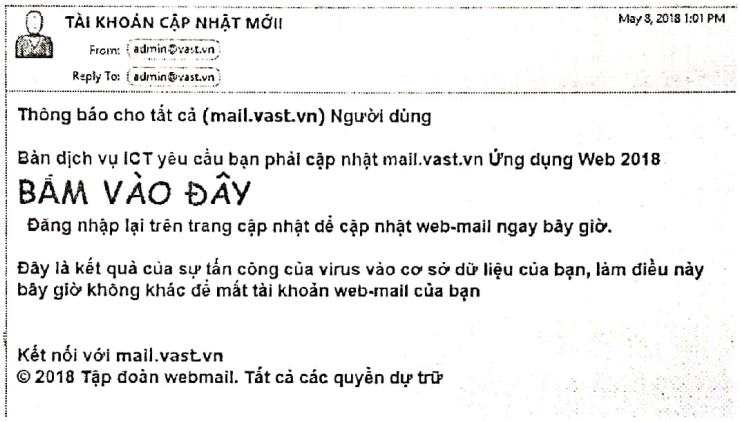
Hướng dẫn phát hiện thư giả mạo trên hệ thống thư điện tử công vụ tại Viện Hàn Lâm Khoa Học và Công Nghệ Việt Nam

(Kèm theo Công văn số 366 /TTTH ngày 19 tháng 9 năm 2019)

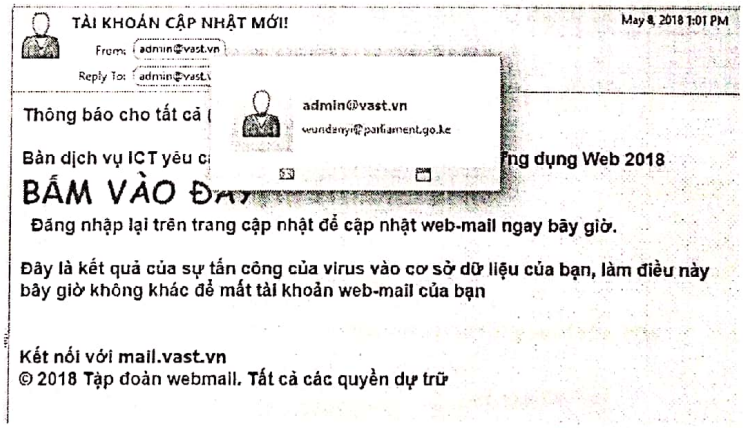
1. Kiểm tra địa chỉ email người gửi

Tin tặc luôn có xu hướng tạo sự tin tưởng với người dùng. Do đó, chúng luôn sử dụng "tên người gửi", hay "tiêu đề" liên quan tới người quản trị và một số yêu cầu cập nhật/nâng cấp hệ thống.

Người dùng có thể dễ dàng kiểm tra địa chỉ gửi bằng cách trỏ chuột vào địa chỉ người gửi.

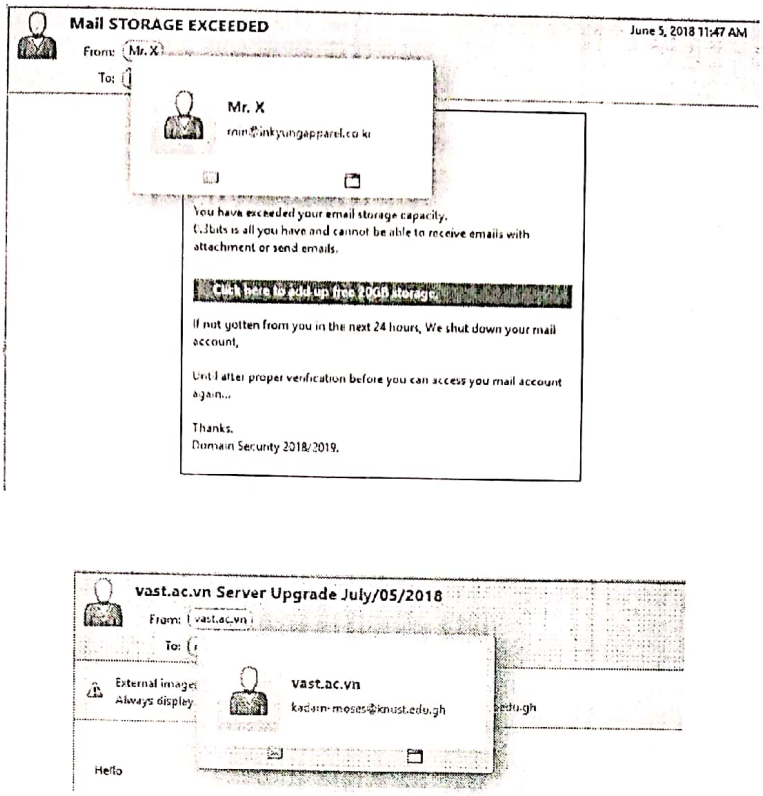


Hình 1. Nội dung Email giả mạo



***Hình 2.** Xác định địa chỉ Email thực sự bằng cách trỏ chuột vào tên người gửi*

Trong trường hợp này, địa chỉ Email thực sự của người gửi là wundanyi@parliament.go.ke, trong khi đó tên hiển thị lại là admin@vast.vn. Đây là hình thức giả mạo tên của người gửi thư điện tử.

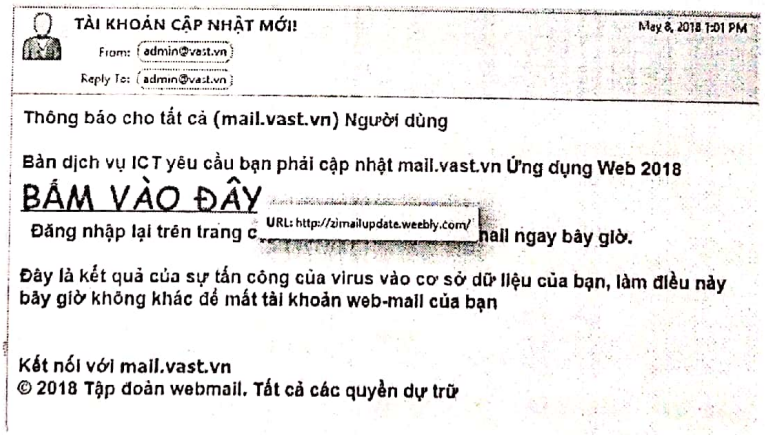


Hình 3. Một ví dụ khác về việc giả mạo

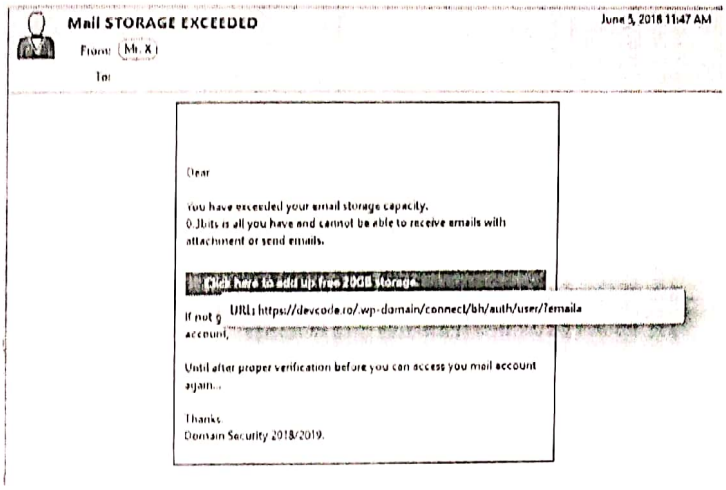
2. Kiểm tra liên kết

Các Email giả mạo thường yêu cầu người dùng nhấn vào các liên kết để đưa người dùng tới các Website chứa virus hay các Website lừa đảo nhằm đánh cắp thông tin/ tài khoản.

Để kiểm tra thực sự đường link chứa trong Email là gì, ta chỉ cần trỏ chuột vào liên kết đó.



Hình 4. Kiểm tra kết nối chứa trong nội dung Email

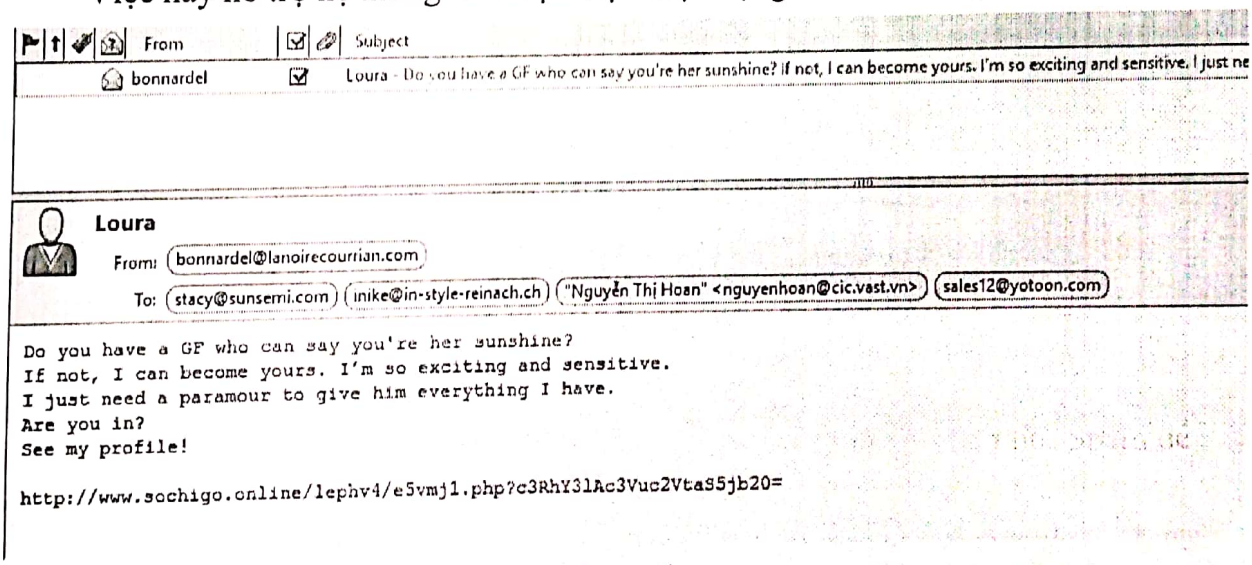


Hình 5. *Kiểm tra kết nối chứa trong nội dung Email*

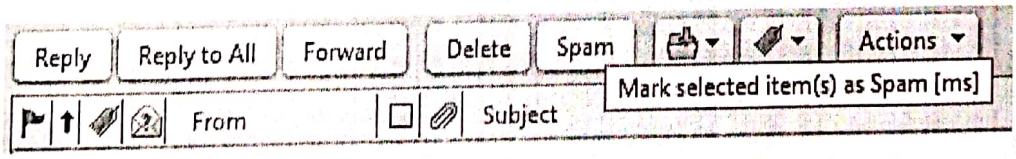
3. Hỗ trợ hệ thống đánh giá phân loại thư rác

Khi nhận được thư mà ta xác định là thư rác, hãy chọn và nhấn nút Spam để chuyển thư này vào mục "Thư rác" (còn gọi là Junk hay Spam)

Việc này hỗ trợ hệ thống cải thiện việc nhận dạng thư rác và ngăn chặn về sau.



Hình 6. *Chọn thư rác để chuyển vào thư mục Spam*



Hình 7. *Nhấn nút Spam để chuyển thư đã chọn vào thư mục Spam*

Việc này sẽ hỗ trợ hệ thống cải thiện việc nhận dạng thư rác và ngăn chặn về sau