MỤC LỤC

Danh mục thuật ngữ và từ viết tắt

STT	Thuật ngữ và từ viết tắt	Giải thích từ ngữ
1	Email	Thư điện tử
2	Email Spam	Thư rác
3	Security	An toàn
4	Mail Client	Phần mềm sử dụng để duyệt thư điện tử như: Outlook Express; Thunder Bird; Ms Office Outlook; Zimbra Desktop; IncrediMail v.v…
5	Operation system (OS)	Hệ điều hành
6	Access point (AP)	Điểm truy cập mạng không dây
7	TĐT CV	Thư điện tử công vụ
8	VNCERT	Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam
9	Hòm thư điện tử công vụ	
10	CA	Trung tâm quản lý chứng chỉ số.
11	Private	Cá nhân, riêng tư

HƯỚNG DẪN SỬ DỤNG AN TOÀN HÒM THƯ ĐIỆN TỬ CÔNG VỤ

I. Đặt vấn đề

Trong thời gian gần đây, thư điện tử đã trở thành một công cụ hữu hiệu trong việc trao đổi thông tin góp phần quan trọng trong việc nâng cao hiệu quả công việc, năng suất lao động, giảm thời gian thực hiện và chi phí hoạt động. Tuy nhiên bên cạnh đó xuất hiện nhiều vấn đề liên quan đến an toàn thông tin như:

- Lộ lọt các thông tin bí mật, nhạy cảm.
- Phát tán các thư giả mạo, có nội dung lừa đảo hoặc quảng cáo không phù hợp.
- Phát tán, lây lan mã độc, phần mềm quảng cáo trái phép v.v….
- Chiếm quyền sử dụng trái phép.
- Bị lợi dụng để phục vụ cho các mục đích xấu.

Các vấn đề trên đã gây ảnh hưởng xấu tới việc sử dụng thư điện tử trong các hoạt động quản lý, trao đổi thông tin. Hướng dẫn dưới đây sẽ đưa ra một số nguyên tắc cơ bản mà người sử dụng hệ thống thư điện tử trong cơ quan nhà nước cần chú ý để sử dụng an toàn, hiệu quả hòm thư điện tử được cấp, tránh bị mất thông tin hoặc bị chiếm quyền sử dụng, lợi dụng cho các mục đích khác.

II. Nguyên tắc chung sử dụng thư điện tử an toàn

Khi sử dụng hòm thư điện tử công vụ (TĐT CV) do cơ quan nhà nước (CNNN) cấp, người sử dụng cần chú ý tuân thủ đầy đủ các nguyên tắc cơ bản sau:

- Hạn chế tối đa việc truy cập hòm thư điện tử bằng các máy tính không đảm bảo toàn hoặc mạng máy tính không an toàn.
- Hạn chế tối đa việc sử dụng máy tính cá nhân truy cập hòm thư điện tử công vụ thông qua các mạng Internet không an toàn như: truy cập mạng Internet thông qua các điểm truy cập không dây tại quán ăn, giải khát, không rõ nguồn gốc v.v..; truy cập mạng Internet thông qua
- Không sử dụng hòm thư điện tử công vụ do cơ quan cấp cho mục đích cá nhân như: đăng ký các dịch vụ thương mại, dịch vụ trao đổi chia sẻ thông tin cá nhân,

- Không đặt chế độ chuyển thư tự động từ hòm thư điện tử công vụ được cấp tới hòm thư khác không phải do các cơ quan nhà nước cấp.

- Hạn chế sử dụng các ứng dụng duyệt thư điện tử có sẵn trên các thiết bị di động như Smart phone hoặc máy tính bảng để truy cập vào các hòm thư điện tử công vụ được cấp.

- Chú ý cảnh giác với những thư điện tử có nội dung, nguồn gốc khả nghi và tiến hành kiểm tra và xử lý thư giả mạo theo hướng đẫn kiểm tra thư giả mạo của Trung tâm VNCERT.

- Đánh dấu Spam ngay khi nhận được các thư rác.

- Khi nhận được thư điện tử gửi kèm tệp tin mà không phát hiện ra nghi ngờ thì thực hiện các bước sau: 1) Tải tệp tin về ổ cứng (tuyệt đối không mở hoặc kích hoạt tệp tin ngay); 2) Dùng phần mềm diệt mã độc quét kiểm tra tệp tin vừa tải về (nếu cần có thể liên lạc lại với người gửi thư để xác nhận tệp tin đã nhận được). Chỉ mở tệp tin nếu không phát hiện ra mã độc; 3) Nếu phát hiện ra mã độc, gửi thư điện tử đó dưới dạng file đính kèm cho quản trị hệ thống và địa chỉ antoanthudientu@report.vncert.vn để xử lý.

- Không gửi, nhận tệp tin thực thi qua hệ thống thư điện tử và hạn chế việc dùng tệp tin nén có mã hóa.

- Khuyến khích sử dụng chữ ký số để ký xác nhận trên thư điện tử gửi đi và kiểm tra nguồn gốc thư điện tử khi tiếp nhận bằng chữ ký số nếu thư đó đã được ký bằng chữ ký số của người gửi.

- Xóa thư khi không còn cần thiết để tránh bị mất mát thông tin nếu tài khoản bị lộ.

- Sử dụng và quản lý mật khẩu theo hướng dẫn sử dụng mật khẩu an toàn do Trung tâm VNCERT cung cấp.

III. Thiết lập môi trường an toàn

III.1 Hệ điều hành

Người sử dụng thực hiện theo các nguyên tắc sau để đảm bảo an toàn cho máy tính:

- Liên tục cập nhật các bản vá bảo mật cho hệ điều hành.

- Cấu hình hệ điều hành cho phép chi có tài khoản người dùng mới được phép truy cập thư mục lưu trữ tin nhắn và tệp tin cấu hình.

- Xoá bỏ các chức năng cho phép thực thi các kịch bản trên Windows nếu không thực sự cần thiết.

- Hiển thị đầy đủ phần mở rộng của tệp tin để không kích hoạt nhầm tập tin thực thi.
- Chỉ cài đặt và sử dụng các phần mềm cũng như hệ điều hành có bản quyền.
- Không chạy các ứng dụng dưới quyền quản trị (Administrator).
- Sử dụng các chức năng mã hoá dữ liệu đề phòng trường hợp bị đánh cắp.

III.2 Cài đặt phần mềm phát hiện và diệt mã độc, tường lửa.

- Cài đặt ứng dụng phát hiện và diệt mã độc, thực hiện kiểm tra toàn bộ các thư điện tử và tệp tin đính kèm ngay khi chúng được tải về.
- Cài đặt tường lửa cá nhân để ngăn chặn máy tính khỏi các truy cập không hợp pháp.

III.3 Đảm bảo an toàn khi truy cập hòm thư điện tử bằng trình duyệt web

A. Truy cập bằng các giao thức an toàn

Trong trường hợp hệ thống thư điện tử cung cấp truy cập thư điện tử bằng hai giao thức HTTPS và HTTP, người sử dụng cần sử dụng giao thức HTTPS thay cho giao thức HTTP.

B. Cấu hình an toàn cho trình duyệt web

Khi truy cập hòm thư điện tử bằng trình duyệt web người dùng cần thực hiện các nguyên tắc sau:

- Tắt môi trường chạy ứng dụng java cho trình duyệt web (JRE)
- Cấm popup, flash.
- Vô hiệu hoá ActiveX
- Không chạy các nội dung động trong email.
- Không tự động tải các ảnh hay thông tin từ xa khi mở email.
- Quét virus ngay khi tải các tệp tin đính kèm về máy tính.
- Ngăn chặn việc chạy javascript nếu không cần thiết.
- Không sử dụng chế độ tự động lưu trữ mật khẩu.

Xem chi tiết hướng dẫn các bước tại Phụ lục A của hướng dẫn.

III.4 Đảm bảo an toàn khi truy cập hòm thư điện tử bằng Mail client

A. Cấu hình truy cập máy chủ an toàn

Để truy cập thư mục email trên máy chủ thư điện tử an toàn người sử dụng cần thiết lập các tính năng:

- Sử dụng các giao thức bảo mật SMTPS, POP3S hoặc IMAPS thay thế cho các giao thức SMTP, POP3 hoặc IMAPS nếu máy chủ thư điện tử có hỗ trợ.

B. Cấu hình các tính năng bảo mật của Mail client

Người dùng cần cấu hình cho Mail client các tính năng sau để nâng cao mức độ an toàn theo hướng dẫn chi tiết trong Phụ lục B của báo cáo, về cơ bản bao gồm các nội dung sau:

- Hạn chế sử dụng chế độ tự động lưu trữ mật khẩu.
- Cấu hình sử dụng giao thức mã hoá để truy cập mailbox.
- Tự động tải về và cập nhật các bản vá cho phần mềm và các plugins.
- Cấm tự động hiển thị nội dung và tải hình ảnh từ xa.
- Cấm thực thi các nội dung động(như hiển thị HTML) trong email.
- Kích hoạt các tính năng cảnh báo email lừa đảo.
- Tự động phát hiện và tiêu diệt phần mềm độc hại trên các thư đến, trước khi chúng được lưu vào máy.
- Chuyển thư rác vào hộp thư rác và tự động xoá sau 14 ngày.

IV. Hướng dẫn sử dụng thư điện tử trong môi trường kém an toàn

IV.1 Sử dụng thư điện tử trong môi trường mạng kém an toàn

Khi người dùng sử dụng máy tính cá nhân của mình tại các địa điểm công cộng hoặc môi trường mạng không tin tưởng, không có khả năng kiểm soát an toàn thì sẽ có các nguy cơ sau:

- Bị nghe lén trên đường truyền dẫn đến mất thông tin đăng nhập, nội dung email.
- Bị giả mạo máy chủ thư điện tử hoặc chuyển hướng đến các trang web giả mạo dẫn đến mất thông tin quan trọng nếu người dùng nhập vào.

Trong trường hợp cần thiết phải truy cập hộp thư điện tử bằng môi trường mạng kém an toàn người dùng phải tuyệt đối tuân theo các nguyên tắc sau để đảm bảo an toàn:

- Người dùng khi truy cập hộp thư điện tử cần sử dụng mạng riêng ảo (VPN) của cơ quan cung cấp để đảm bảo an toàn.
- Trong trường hợp không có VPN thì người dùng phải sử dụng đường truyền được mã hoá SSL/TLS, ví dụ như truy cập web mail sử dụng HTTPS, nhận thư sử dụng POP3S, IMAPS, gửi thư sử dụng SMTPS.

- Khi sử dụng mã hoá SSL/TLS phải chú ý kiểm tra chữ ký điện tử của máy chủ thư điện tử trong trường hợp các chữ ký bị cảnh báo để tránh bị giả mạo chữ ký điện tử. Phụ lục C hướng dẫn kiểm tra chữ ký điện tử của máy chủ thư điện tử.
- Trong trường hợp máy chủ thư điện tử không cung cấp mã hoá đường truyền, người sử dụng phải sử dụng phương pháp truy cập khác gián tiếp mà an toàn như việc truy cập an toàn đến một máy tính cá nhân ở cơ quan hoặc ở nhà. Sau đó từ máy tính này truy cập đến máy chủ thư điện tử để sử dụng email.

Nếu người dùng không tuân theo các quy tắc trên thì việc mất mát thông tin email sẽ dẫn đến nhiều hậu quả nghiêm trọng cả cho cá nhân và hệ thống thư điện tử.

IV.2 Sử dụng thư điện tử trên máy tính dùng chung

Việc sử dụng thư điện tử tại máy tính dùng chung sẽ dẫn đến các nguy cơ sau:

- Mắc phải các nguy cơ tương tự như việc sử dụng thư điện tử tại môi trường mạng kém an toàn trong phần IV.1.
- Nguy cơ bị cài, cắm các phần mềm độc hại trong máy tính như phần mềm ghi lại thao tác bàn phím, phần mềm chụp ảnh màn hình hay phần mềm đánh cắp dữ liệu...
- Nguy cơ khi bị tự động lưu trữ mật khẩu và dữ liệu trên các máy tính này, việc này dễ dàng bị khai thác bởi người khác cùng sử dụng máy tính này.

Trong môi trường kém an toàn, người dùng phải hạn chế tối đa sử dụng thư điện tử. Trong trường hợp bắt buộc phải sử dụng, người dùng có thể dùng các biện pháp sau để hạn chế tối thiểu thiệt hại :

- Người dùng có thể dùng cách biện pháp trong phần V.1 để đảm bảo an toàn cho môi trường mạng. Ngoài ra các biện pháp sau đây sẽ tăng thêm mức độ an toàn cho người dùng.
- Tiến hành kiểm tra máy tính không an toàn bằng cách tải bản mới nhất của phần mềm điệt virus phiên bản rút gọn từ internet. Có nhiều phần mềm diệt virus miễn phí như Avira, Avast...
- Người dùng có thể sử dụng bàn phím ảo để tránh việc bị keylogger đánh cắp mật khẩu. Nhưng việc này bị vô hiệu nếu máy tính đó cũng bị cài phần mềm chụp ảnh màn hình. Việc kết hợp sử dụng bàn phím vật lý và bàn phím ảo, mã hoá đường truyền sẽ hạn chế việc bị đánh cắp mật khẩu trong môi trường không an toàn. Phụ lục D hướng dẫn bật bàn phím ảo trong các hệ điều hành.

- Tuyệt đối không lưu trữ mật khẩu trên trình duyệt hay phần mềm trên máy tính công cộng. Nên sử dụng chế độ private brower của các trình duyệt để không lưu lại các thông tin và dữ liệu truy cập của cá nhân. Phụ lục E hướng dẫn sử dụng trình duyệt ở chế độ private.

Các biện pháp trên chỉ hạn chế các nguy cơ khi sử dụng thư điện tử trong môi trường kém an toàn chứ không thể hoàn toàn đảm bảo an toàn cho người dùng.

IV.3 Sử dụng thư điện tử công vụ khi đi công tác nước ngoài:

Đối với các cán bộ đi công tác nước ngoài thì có một số điểm đặc biệt cần chú ý để hạn chế mất mát thông tin cũng như bị lây nhiễm mã độc như sau:

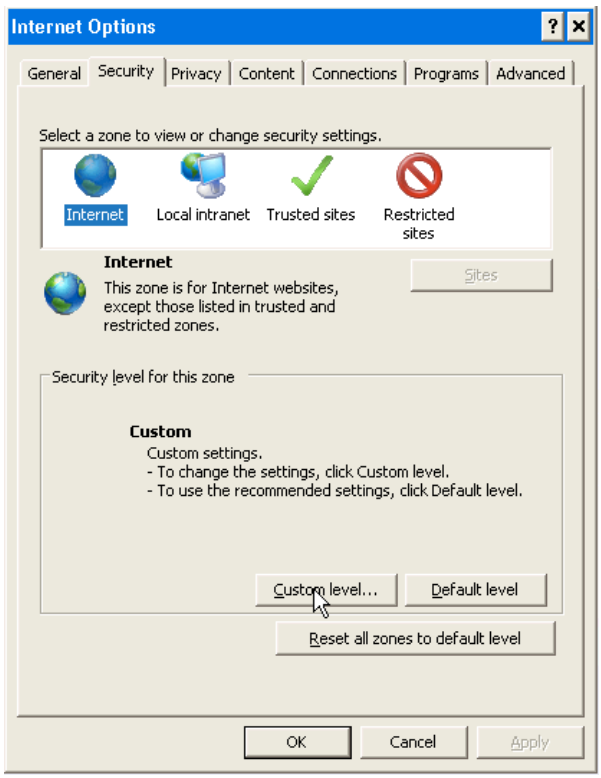
- Nên sử dụng máy tính dành riêng cho mục đích đi công tác để tránh bị đánh cắp thông tin và khi về có thể giao cho bộ phận kỹ thuật kiểm tra mã độc hoặc phần mềm gián điệp.
- Yêu cầu nhân viên kỹ thuật cung cấp dịch vụ VPN để kết nối bảo mật về đơn vị, từ đó kết nối ra internet để tránh bị theo dõi nội dung làm việc.
- Sử dụng tài khoản thư điện tử tạm thời trong thời gian đi công tác và không sử dụng thư điện tử công vụ cho các mục đích cá nhân.
- Thay đổi toàn bộ các mật khẩu của các tài khoản đã sử dụng khi đi công tác và cả các mật khẩu của các tài khoản không sử dụng nhưng trùng với các mật khẩu đã sử dụng.
- Khi truy cập internet từ các điểm công cộng (như sân bay, nhà ga...) mà không phải khai báo danh tính sẽ ít nguy cơ bị theo dõi hơn là khi truy cập từ phòng riêng khách sạn hay những nơi phải khai báo danh tính để truy cập internet. Tuy nhiên nguy cơ lây nhiễm mã độc thì không giảm.

Ngoài ra các cán bộ đi công tác cần chú ý thực hiện theo mục IV.1, IV.2 để đảm bảo không bị nghe lén hoặc giả mạo máy chủ thư điện tử.

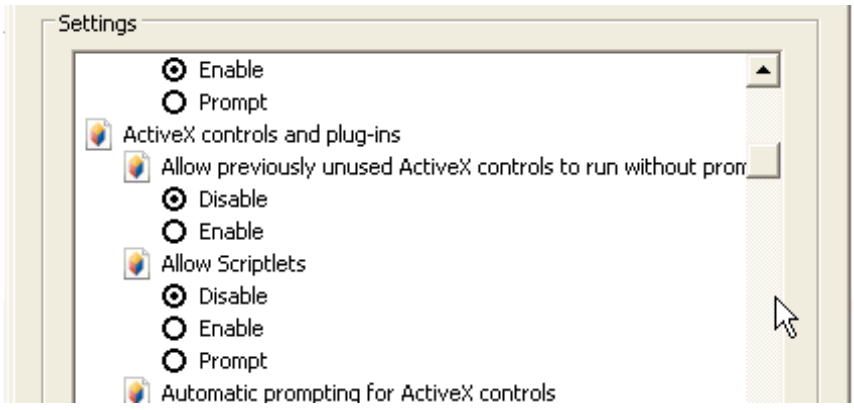
Phụ lục A: Hướng dẫn cấu hình bảo mật cho trình duyệt Web.

A.1 Internet Explorer

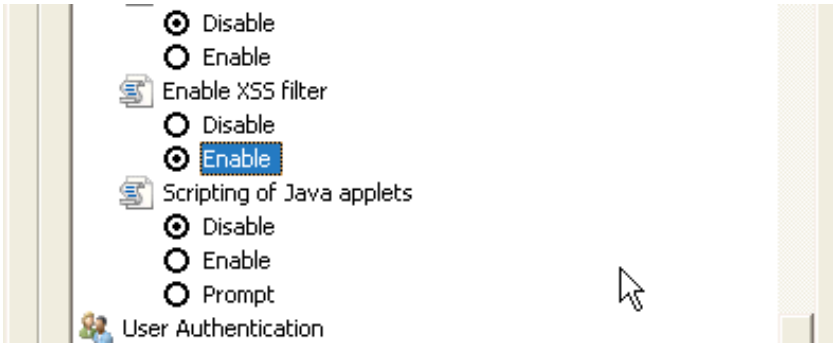
Bước 1. Để cấu hình các thông tin bảo mật cho Internet Explorer ta truy cập vào bảng Internet Options (Tools-> Internet Options), chọn tab Security -> Custom level:



Bước 2. Tiếp theo người dùng cần cấu hình các chức năng Vô hiệu hoá ActiveX bằng cách lựa chọn Disable trong mục "Allow previously unused ActiveX control to run without promt" và "Allow Scriptlets".

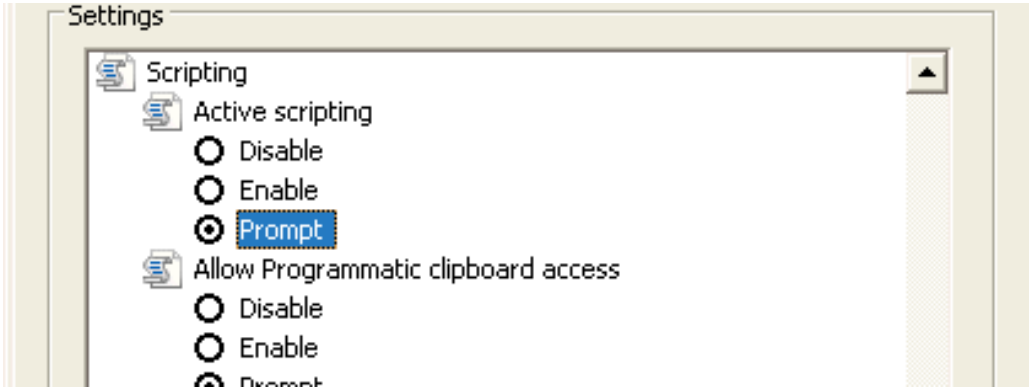


Bước 3. Và kích hoạt tính năng filter XSS trong mục enable XSS filter như hình dưới:



Bước 4. Người sử dụng có thể kích hoạt tính năng chặn Pop-up bằng cách tích vào ô Enable trong mục Use Pop-up Blocker như sau:

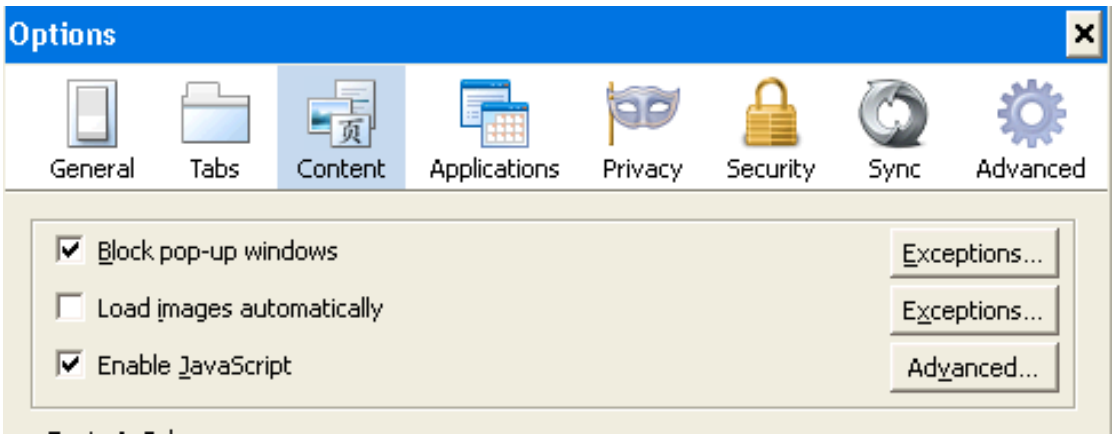
Bước 5. Tích vào "Prompt" trong mục "Active scripting" để yêu cầu hỏi khi chạy các kịch bản động.



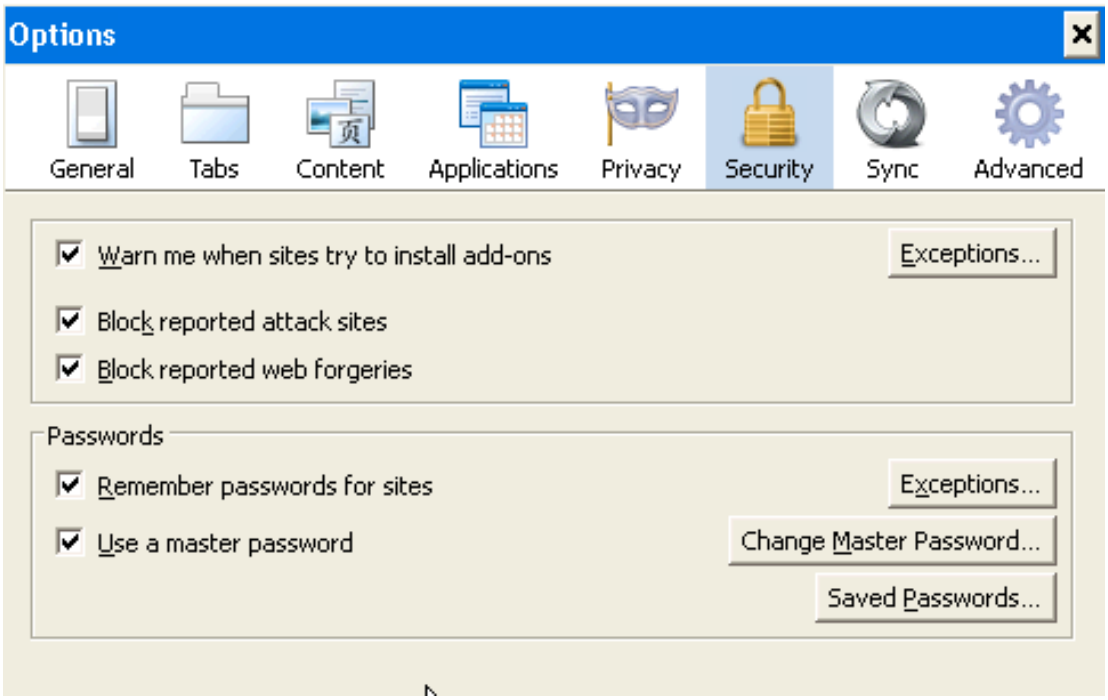
A.2 Mozillar/Firefox

Tương tự như trên IE, trên Firefox người dùng cũng thiết lập một số tính năng bằng cách truy cập vào Options->options:

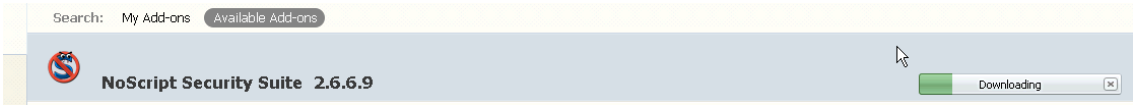
Bước 1. Kích hoạt tính năng chặn pop-up và vô hiệu hoá việc tải hình ảnh tự động(tích vào ô Block Pop-up window).



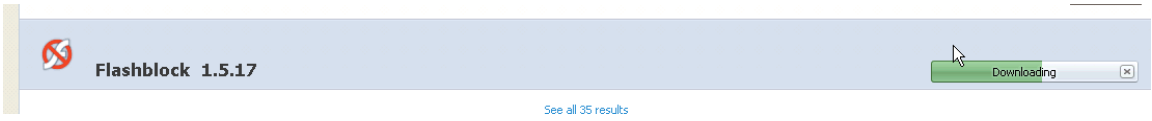
Bước 2. Bỏ thiết lập lưu mật khẩu trên trình duyệt bằng cách bỏ tích ở ô "Remember passwords for sites" ở tab Security:



Bước 3. Người dùng cần vào mục FireFox -> Addons để cài đặt hoặc quản lý addons. Thực hiện cài addons "NoScript" để ngăn chặn việc thực thi các script ngầm mà ta không biết:



Bước 4. Cài addons Flashblock để ngăn chặn việc chạy ngầm các flash hoặc các quảng cáo khó chịu:

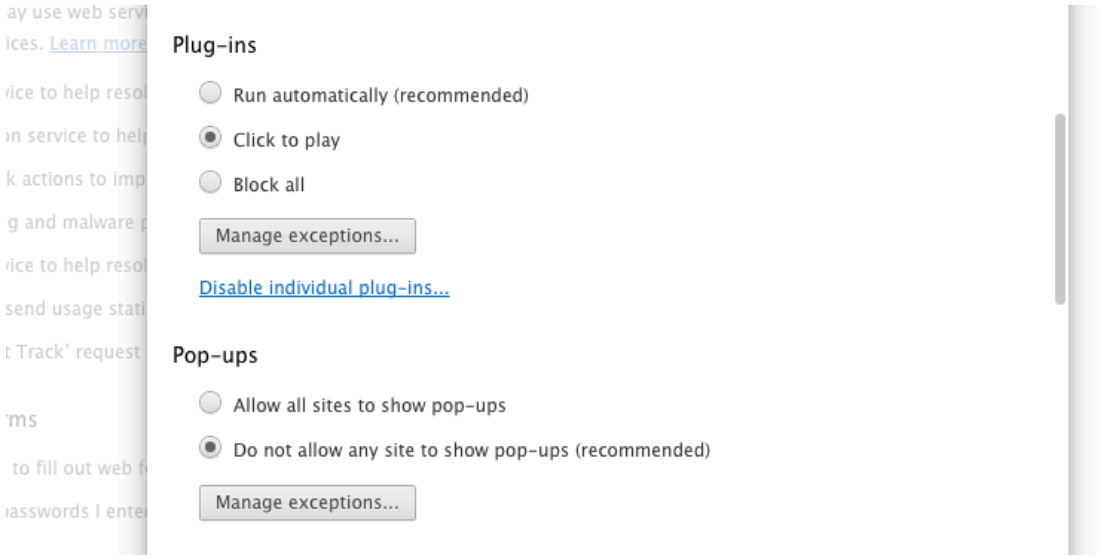


A.3 Google Chrome

Chrome cũng tương tự như Firefox, ngoài các cấu hình thiết lập ta có thể cài đặt các tiện ích mở rộng để nâng cao bảo mật.

Truy cập link: "chrome://settings/content" để cấu hình bảo mật cho Chrome.

Cấu hình ngăn chặn việc chạy tự động các flash và bật popup ở đây(Chọn Click to play để yêu cầu hỏi mỗi khi chạy flash. Điều này giúp người dùng tránh khỏi những flash ngoài ý muốn):

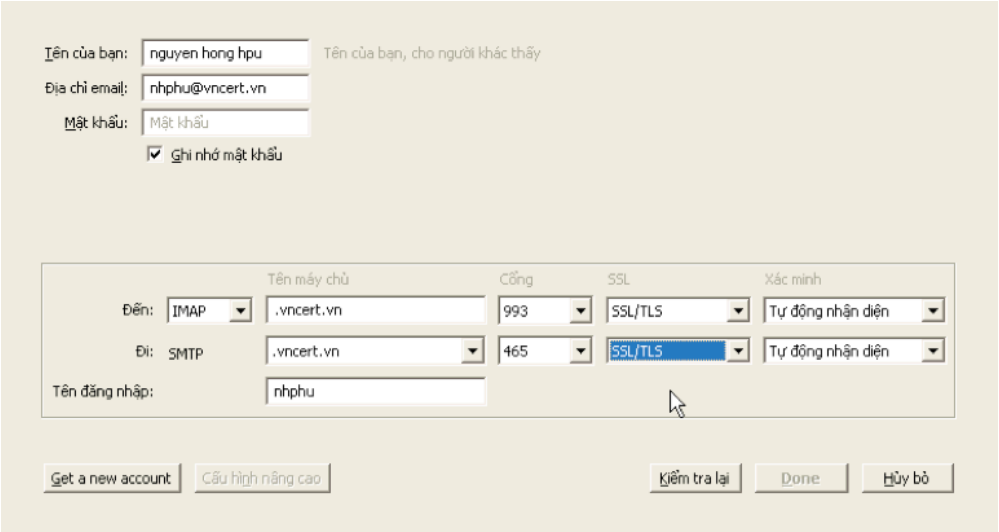


Ngoài ra người dùng cũng có thể cài đặt thêm các tính năng mở rộng tương tự Firefox như Script Blocker, Flash Control.

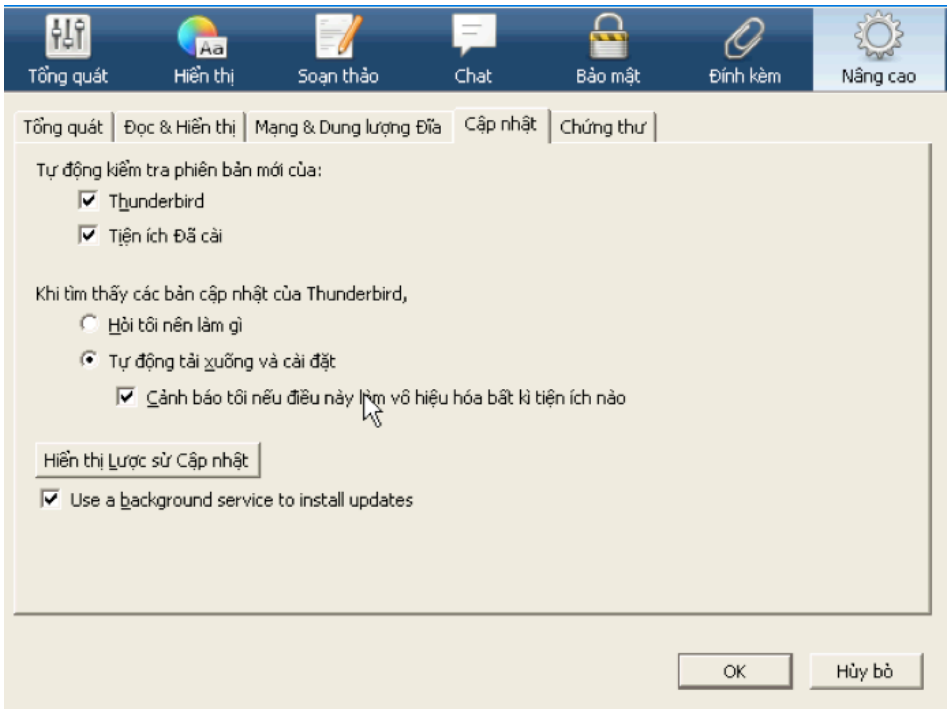
Phụ lục B: Hướng dẫn cấu hình an toàn cho ứng dụng Mail Client

B.1 Ứng dụng Mozilla/Thunderbird

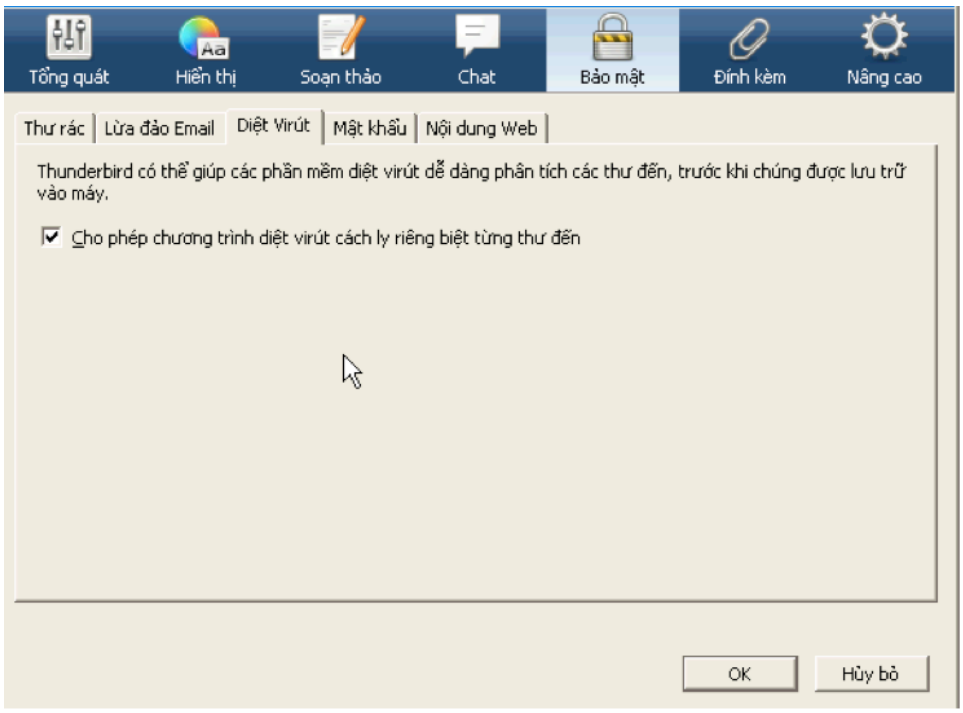
Bước 1. Để thêm tài khoản email vào ứng dụng email client người dùng cần cấu hình thông số để truy cập máy chủ thư điện tử. Khi cấu hình cần lựa chọn phương thức truy cập máy chủ thư mã hoá. Trong thiết lập tài khoản người sử dụng điền thông tin sử dụng mã hoá SSL/TLS trong ô SSL cho cả thư đến và thư đi như trong hình:



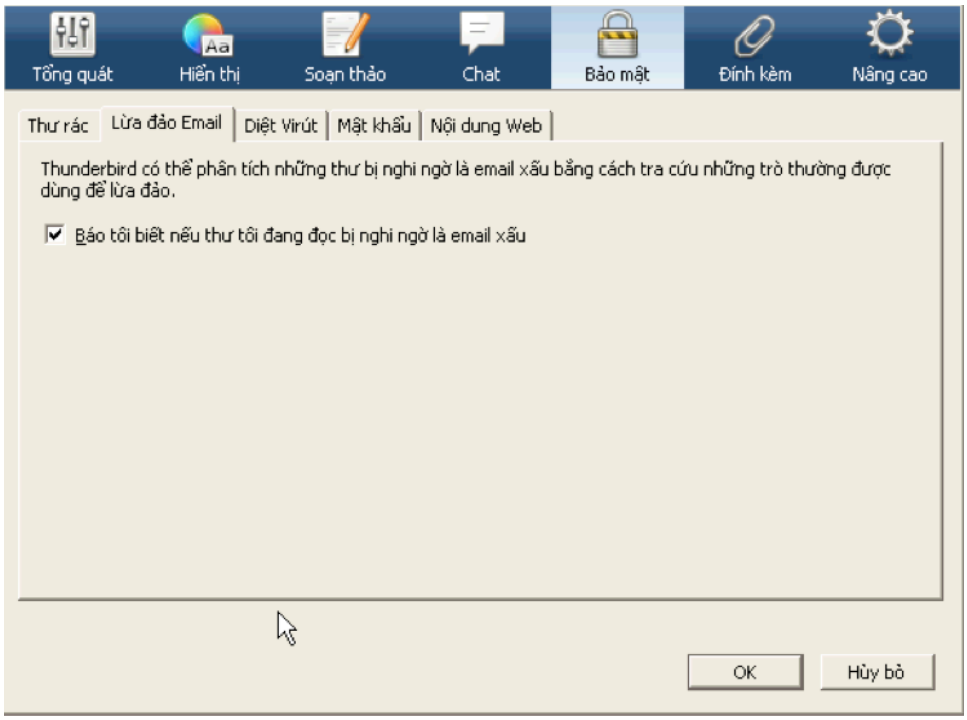
Bước 2. Để thiết lập các cấu hình khác người dùng vào phần Tools->Options -> Security(Công cụ -> Tuỳ chọn->Bảo Mật). Thiết lập tự động kiểm tra phiên bản mới của Thunderbird và các tiện ích cần được lựa chọn ở trong tab Nâng cao-> Tổng quát.



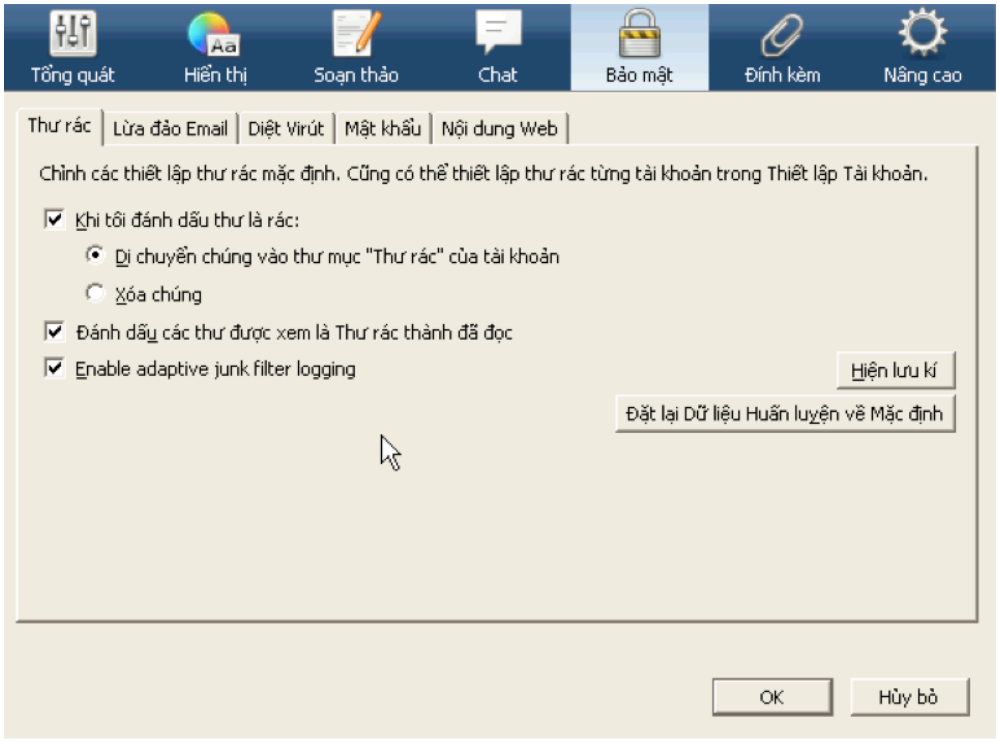
Bước 3. Lựa chọn thiết lập diệt virus các thư điện tử gửi đến trước khi lưu trữ vào hệ thống bằng cách lựa chọn trong tab Bảo mật -> Diệt virut.



Bước 4. Thiết lập tính năng cảnh báo email xấu nếu bin nghi ngờ ở trong tab "Bảo mật -> Lừa đảo Email"

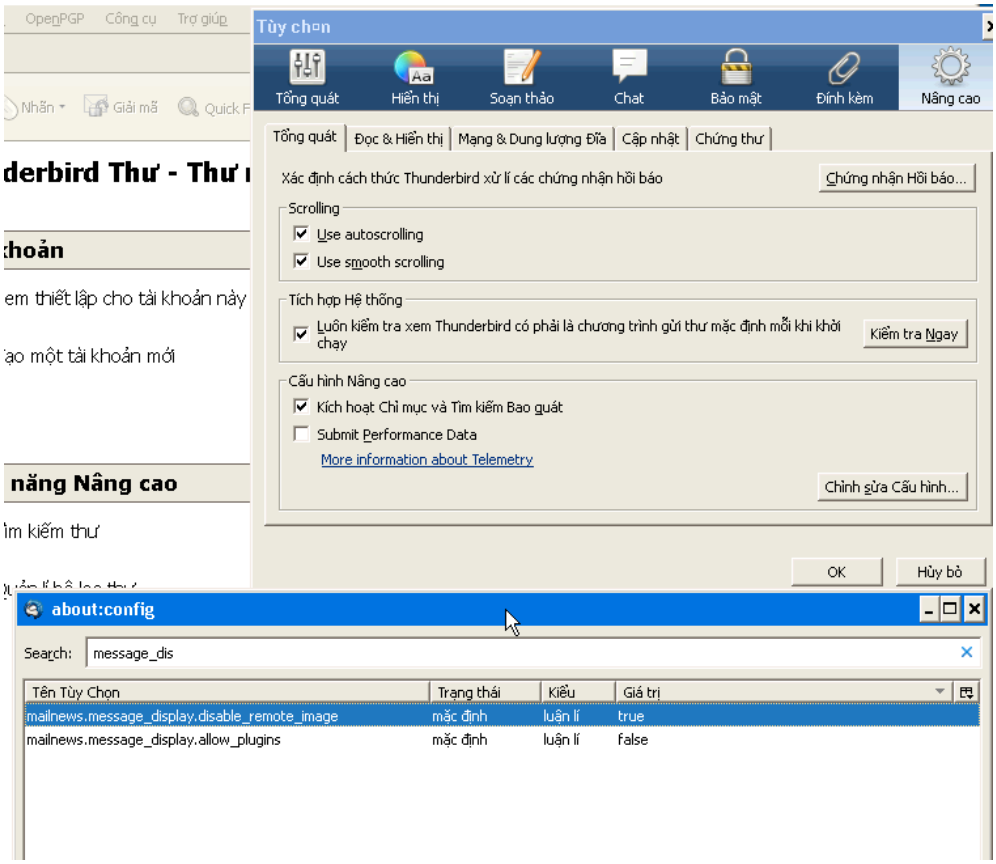


Bước 5. Kích hoạt tính năng đánh đấu và lọc thư rác ở trong tab "Bảo mật -> Thư rác":

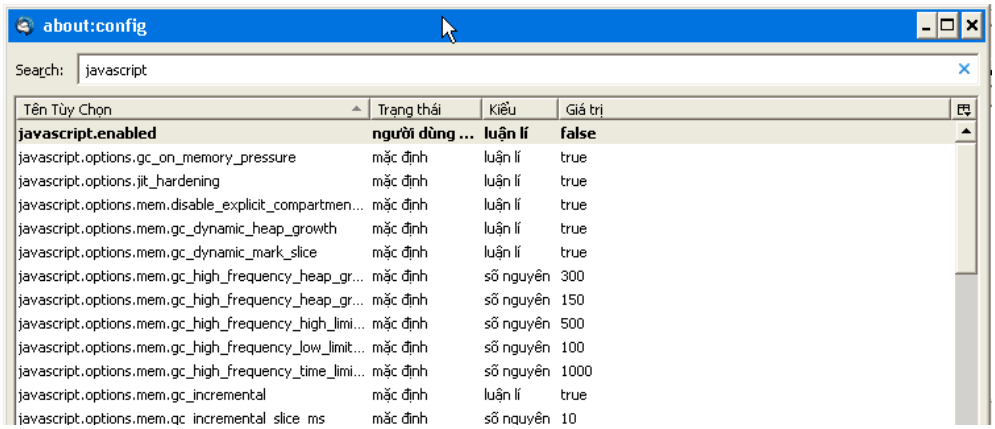


Bước 6. Một số tính năng nâng cao khác yêu cầu người dùng truy cập vào tab Nâng cao -> Chỉnh sửa cấu hình:

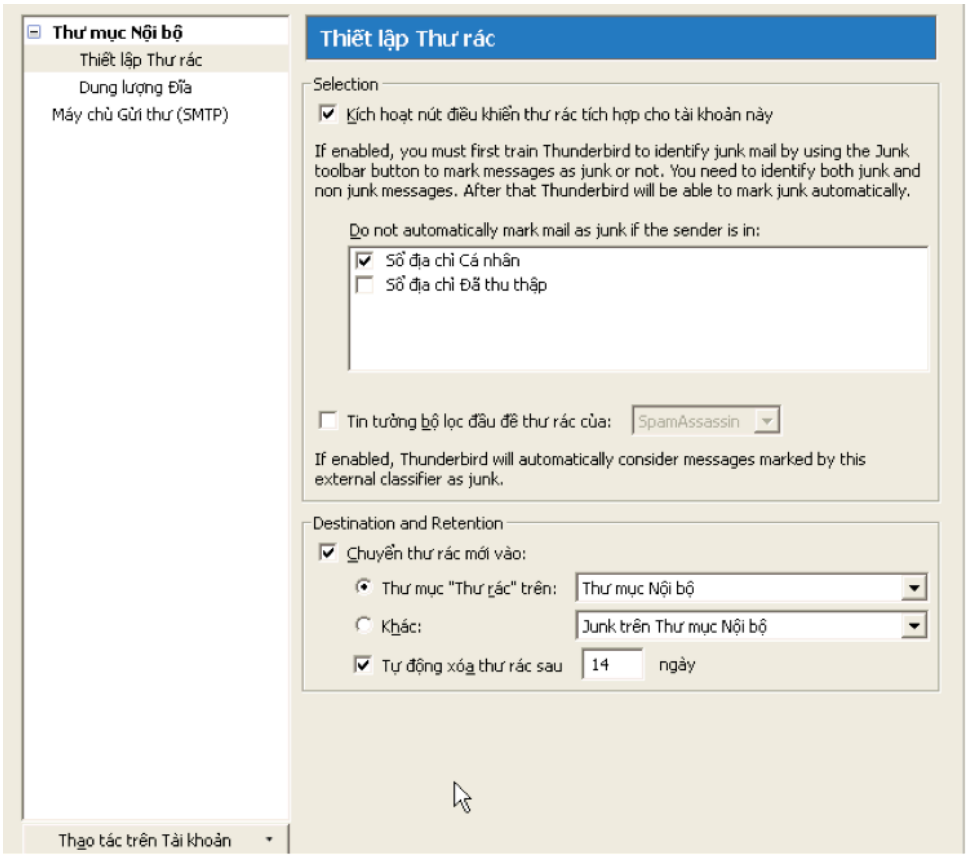
Tìm kiếm các cấu hình "*mailnews.message_display*" ta sẽ thấy tính năng "*mailnews.message_display.disable_remote_image*". Người dùng cần thiết lập giá trị **true**.



Tìm kiếm từ khoá "javascript.enacled" sau đó lựa trọn giá trị false trong biến "javascript.enabled":

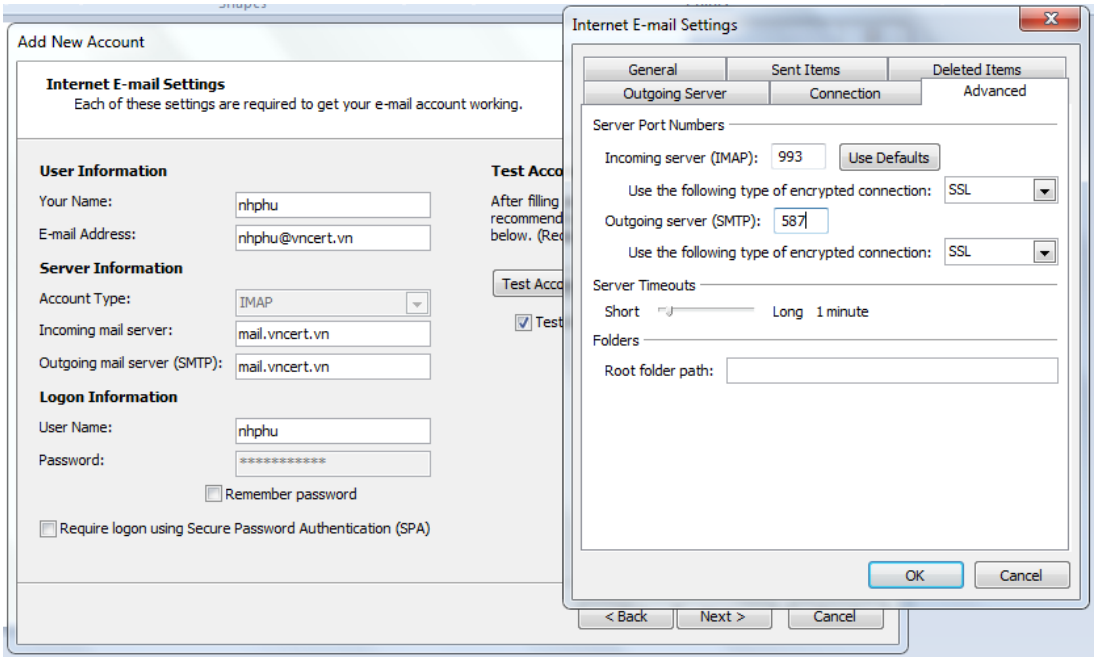


Bước 7. Bước cuối cùng, người dùng vào phần "Công cụ -> Thiết lập tài khoản -> Thư mục nội bộ -> Thiết lập Thư rác". Tại đây người dùng kích hoạt tính năng chuyển thư rác vào thư mục nội bộ và tự động xoá sau 14 ngày để tự động xoá bỏ các thư rác.

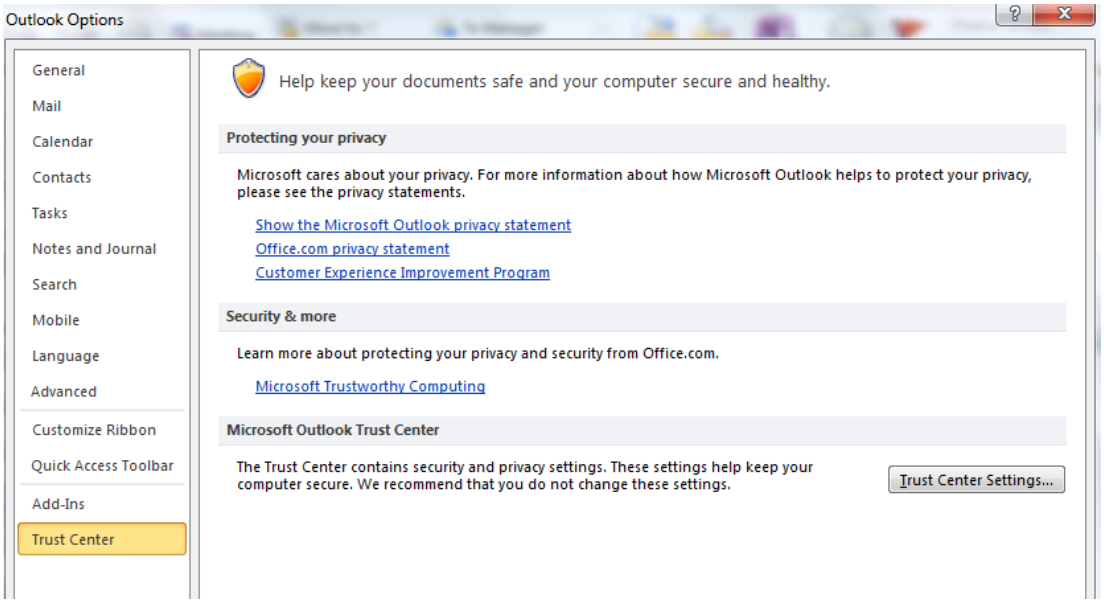


B.2 Ứng dụng Microsoft Outlook 2010

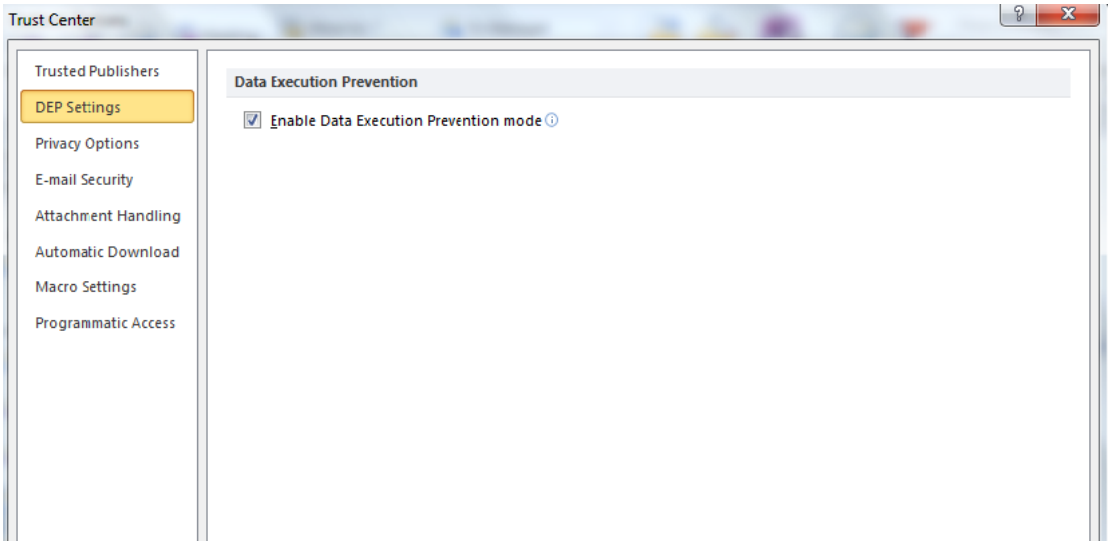
Bước 1. Bước đầu tiên người sử dụng cần thiết lập kết nối an toàn đến máy chủ thư điện tử bằng việc lựa chọn phương thức truy cập có mã hóa SSL như SMTPS, POP3S, IMAPS. Trong thiết lập tài khoản mới cho ứng dụng Outlook, người dùng lựa chọn các thông số kết nối cho tài khoản trong thiết lập Internet Email Settings. Trong tab "Advanced" người dùng lựa chọn giao thức gửi thư đi là SMTPS có mã hoá SSL cổng 465 hoặc 587, giao thức nhận thư là IMAP hoặc POP3 sử dụng mã hoá SSL cổng 993 hoặc 995.



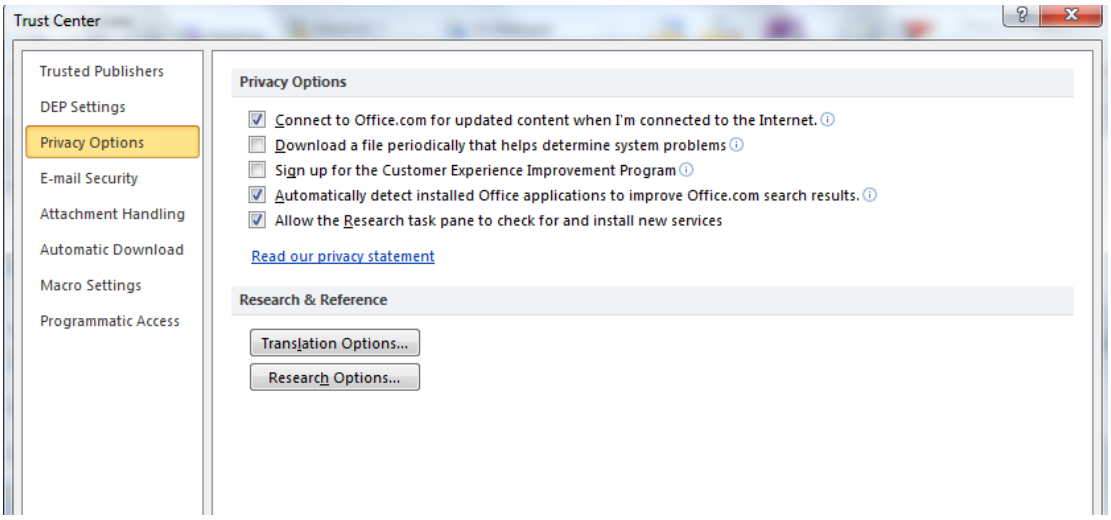
Bước 2. Để cấu hình các tính năng bảo mật cho Outlook người dùng truy cập vào menu: Files-> Options -> Trus Center.-> Trust Center Settings..



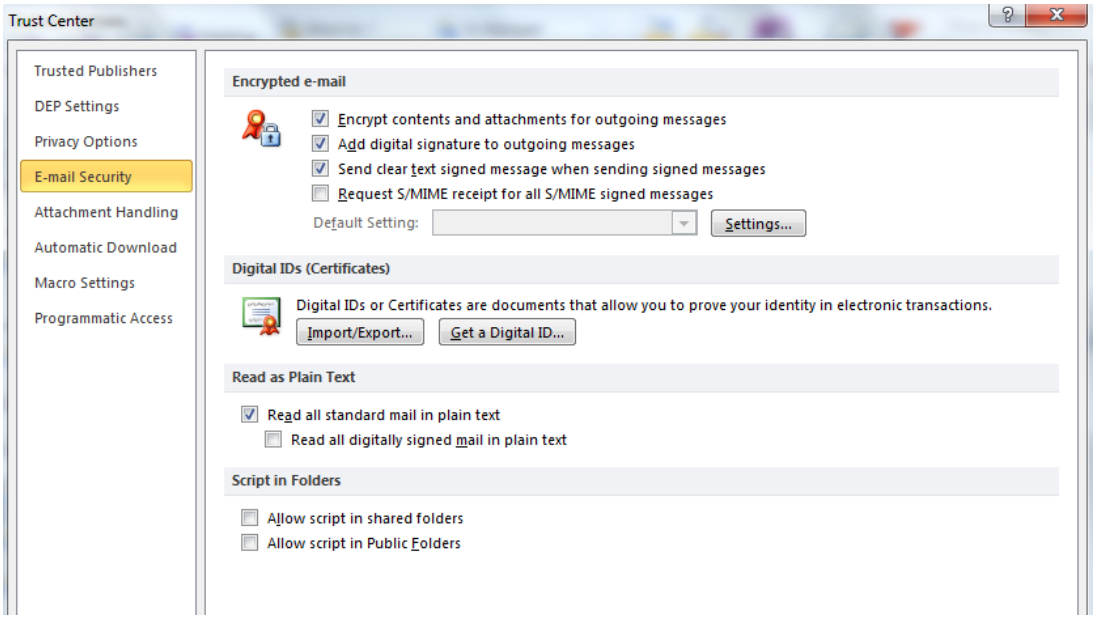
Trong cửa sổ Trust Center ta cấu hình tính năng ngăn chặn thực thi dữ liệu: DEP Settings -> Data Execution Prevention: Tích vào ô "Enable Data Execution Prevention mode"



Bước 3. Tiếp theo là tính năng tự động cập nhật, phát hiện các ứng dụng Office và các phần mềm liên quan mới cài đặt trong tab Privacy Options. Lựa chọn các mục "Connect to Ofice.com for updated...." và "Automatically detect installed..." .

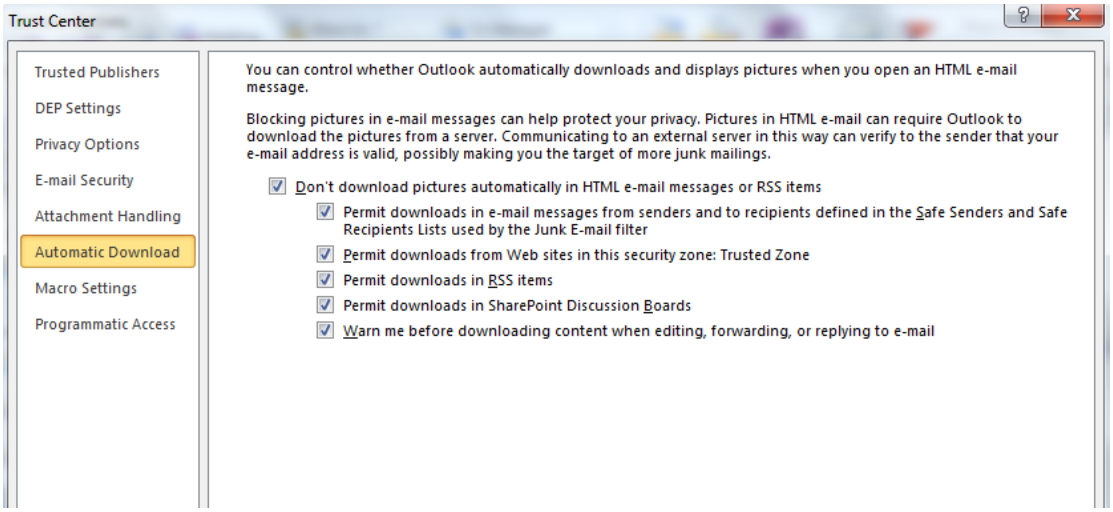


Bước 4. Để đảm bảo an toàn về nội dung cũng như tính chính xác của người gửi ta có thể cấu hình mã hóa nội dung email hoặc ký chữ ký điện tử lên email ở trong tab E-mail Security(lựa chọn tính năng "Encrypt contents and attachments..." và "Add digital signature.." trong tab E-mail Security):

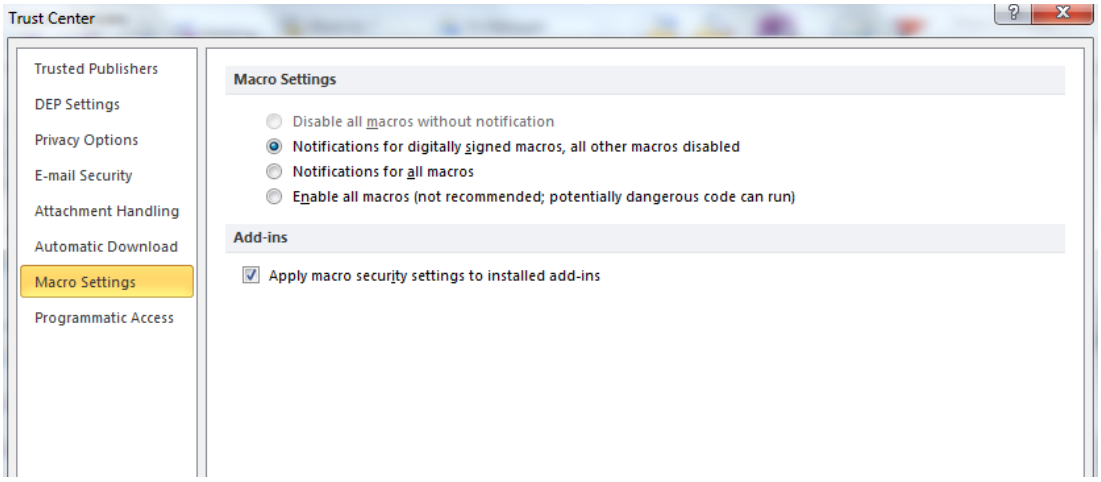


Bước 5. Một phần rất quan trọng trong các email client đó là việc cấu hình tự động hiển thị nội dung động hoặc tải hình ảnh. Cấu hình không cho phép tự động thực hiện các việc đó mà phải hỏi ý kiến người dùng. Để thuận tiện ta có thể tự động với một số địa chỉ tin cậy được nhập vào Trusted zone hoặc Safe Senders:

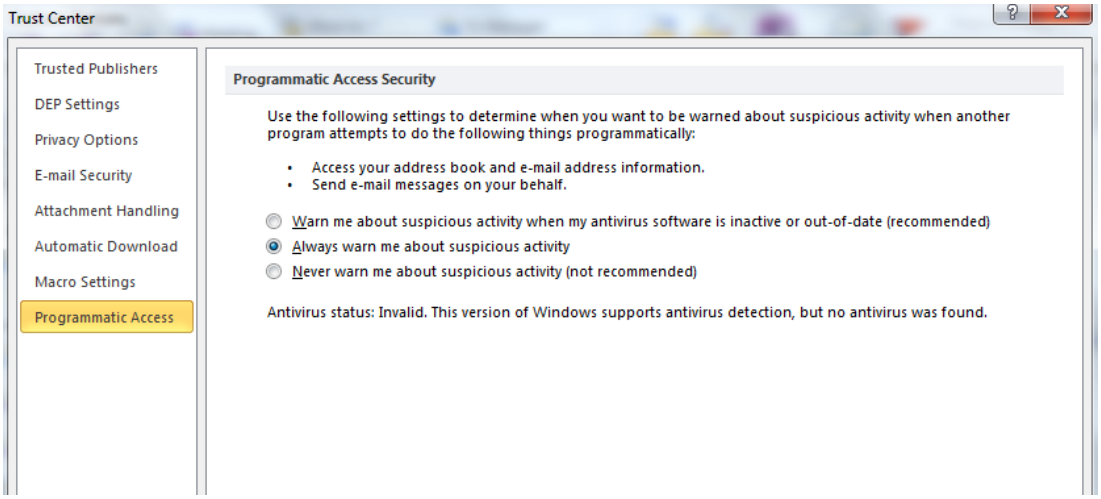
Lựa chọn tính năng "Don't download pictures automatically in HTML e-mail messages or RSS items" trong tab "Automatic Download". Các lựa chọn khác để thêm tính cơ động trong sử dụng. Người dùng có thể lựa chọn hoặc không.



Bước 6. Thiết lập cảnh bảo khi có các macros. Để có chế độ bảo mật cao thì người dùng cần thiết lập cảnh báo với tất cả các macros có chữ ký và vô hiệu hóa các macros khác: Lựa chọn mục "Notification for digitally signed macros, all other macros disabled" trong tab Macro Settings.



Bước 7. Cuối cùng, người dùng cần thiết lập luôn cảnh báo cách hoạt động đáng ngờ ở mục "Always warn me about suspicious activity" ở tab "Programmatic Access":

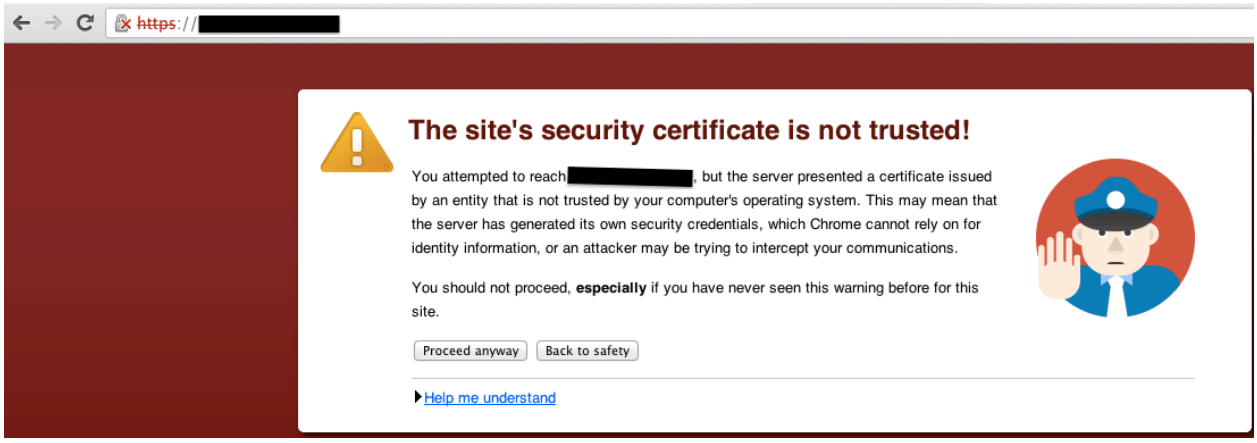


Phụ lục C: Hướng dẫn kiểm tra chứng chỉ số của máy chủ thư

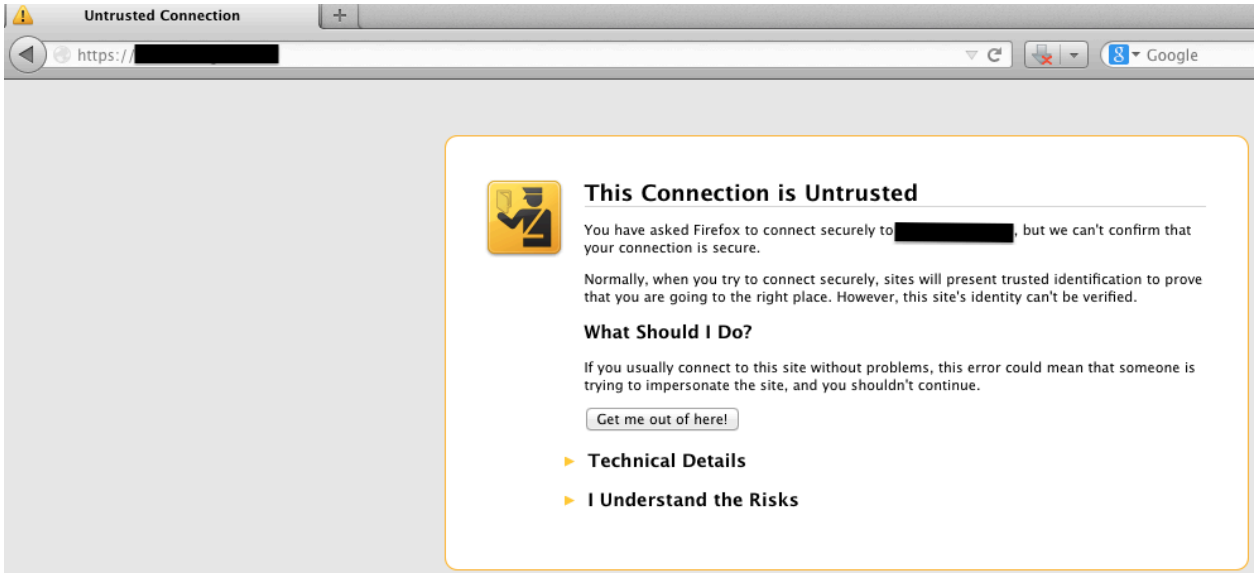
Đối với một số trang web sử dụng kết nối mã hoá SSL/TLS mà không được các CAs công nhận chứng chỉ số thì người dùng phải tự kiểm tra thủ công bằng cách sau:

Bước 1. Xác nhận mã MD5 hoặc SHA1 của chứng chỉ số từ quản trị hệ thống. Đây là mã băm của chứng chỉ số và là duy nhất. Lưu lại mã MD5 và SHA1 lại để tiện theo dõi về sau.

Bước 2. Khi truy cập máy chủ thư điện tử sử dụng kết nối SSL/TLS, vì chứng chỉ số không được các CAs công nhận nên sẽ có các cảnh báo như sau:



Giao diện cảnh báo chứng chỉ số không được xác thực trên Chrome.



Giao diện cảnh báo chứng chỉ số không được xác thực trên FireFox.

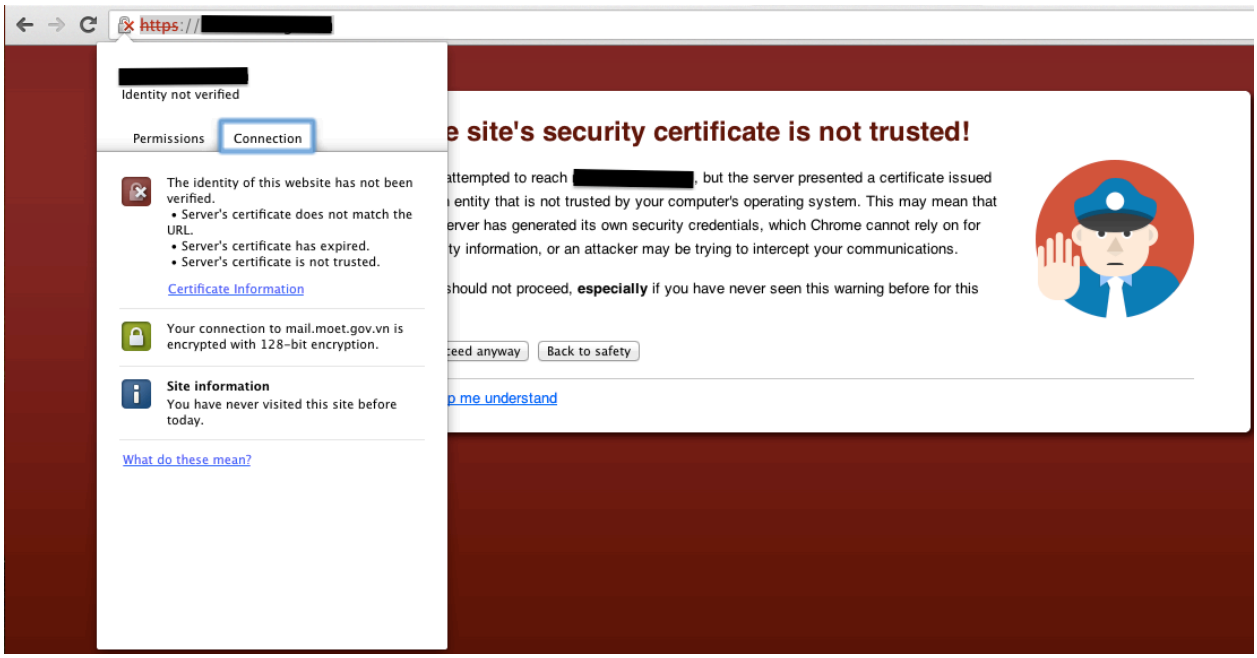
Người sử dụng sẽ nhận được các cảnh báo trên khi truy cập webmail bằng HTTPS lần đầu tiên hoặc khi máy chủ thư điện tử bị thay đổi chữ ký. Trong trường hợp này, người dùng cần phải kiểm tra bằng cách xác nhận mã MD5

hoặc SHA1 của chứng chỉ số với mã băm đã nhận được từ quản trị hệ thống. Cách kiểm tra mã băm của chứng chỉ số được thực hiện như sau:

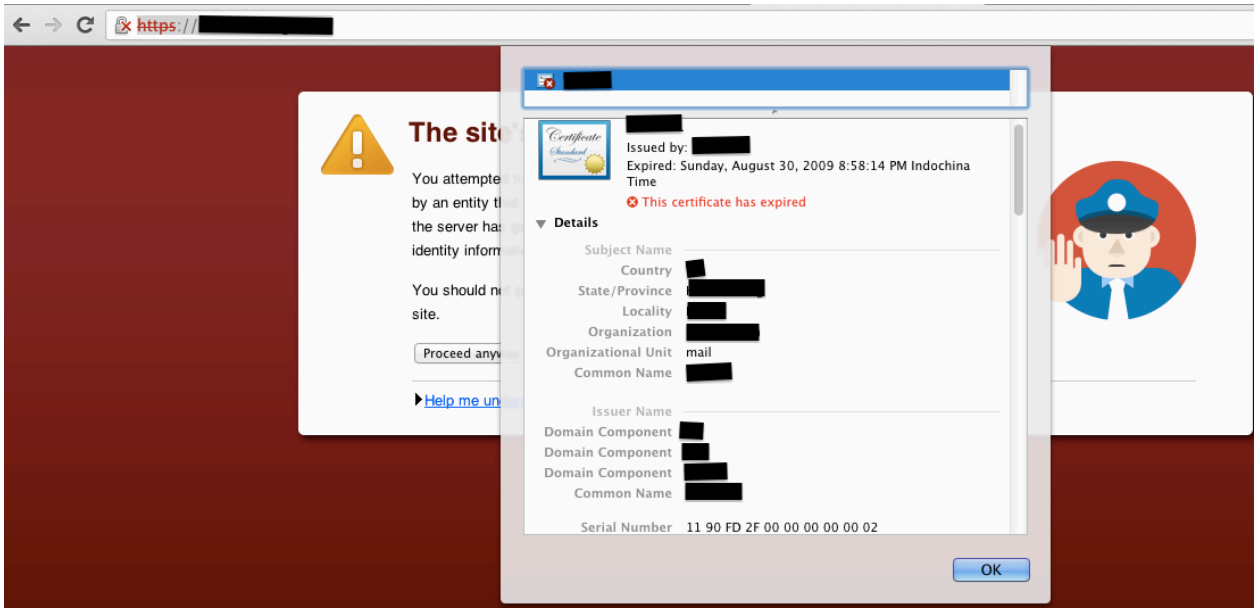
Bước 3.

Đối với trình duyệt Chrome:

Nhấn trái vào biểu tượng khoá có dấu gạch x ở góc trên bên trái trình duyệt. Chọn tab Connection:

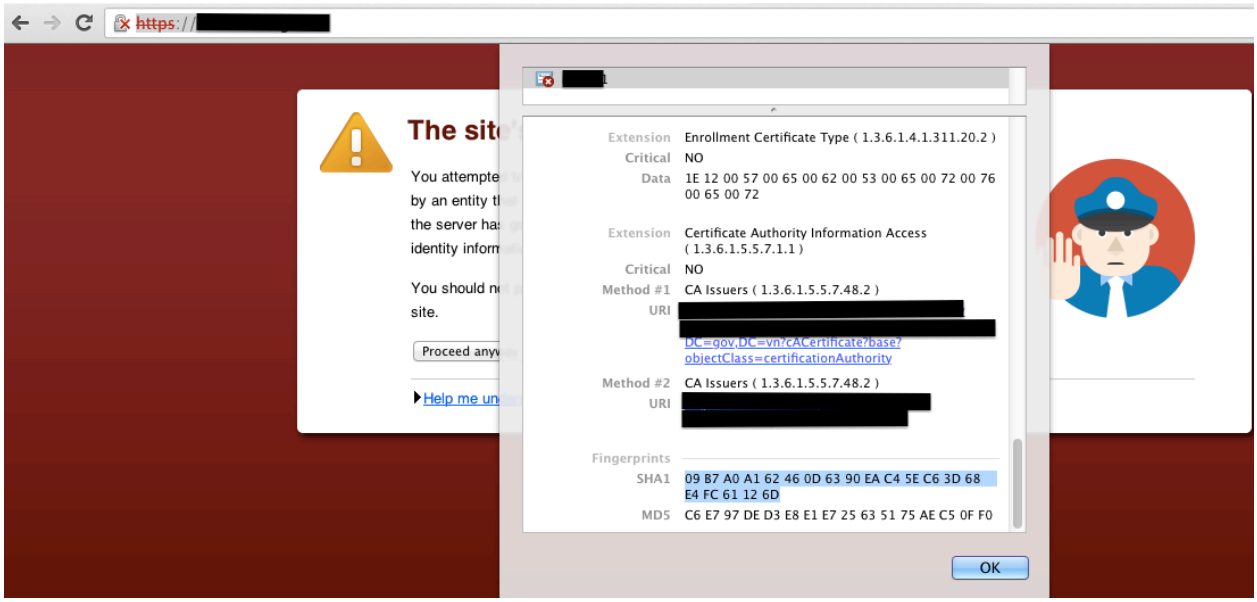


chọn link Certification Information sẽ hiện thị bảng thông tin chứng chỉ:

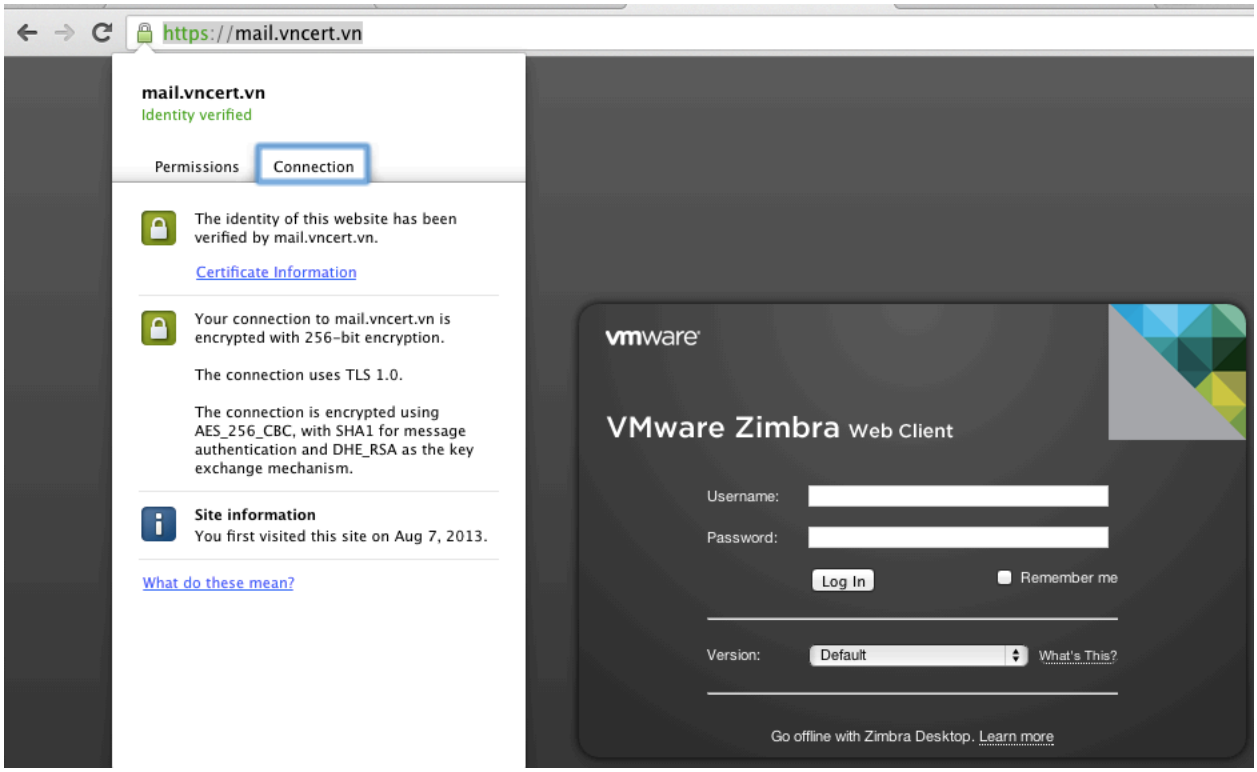


Kéo thanh trượt của bảng thông tin xuống dưới cùng người dùng sẽ thấy thông tin mã băm SHA1 và MD5 của chứng chỉ số. So sánh 2 mã này với thông

tin từ quản trị hệ thống. Nếu 2 mã này trùng nhau thì chứng chỉ là hợp lệ còn không thì chứng chỉ bị giả mạo hoặc đã bị thay đổi.



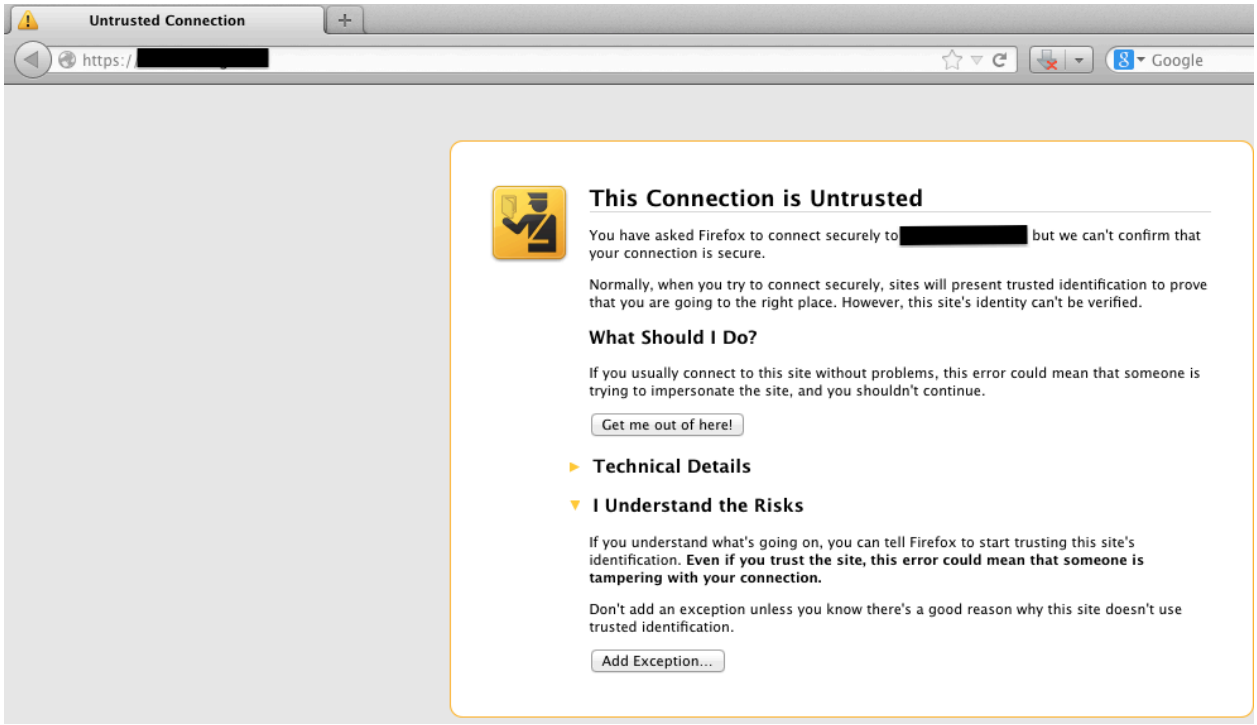
Trong trường hợp chứng chỉ số không hợp lệ người dùng không được truy cập vào máy chủ để tránh bị giảo mạo chứng chỉ và đánh cắp thông tin. Trong trường hợp chứng chỉ số hợp lệ, người dùng nhấn OK và chọn "Proceed anyway" để cài đặt chứng chỉ vào hệ thống và sử dụng đường truyền mã hoá để truy cập:



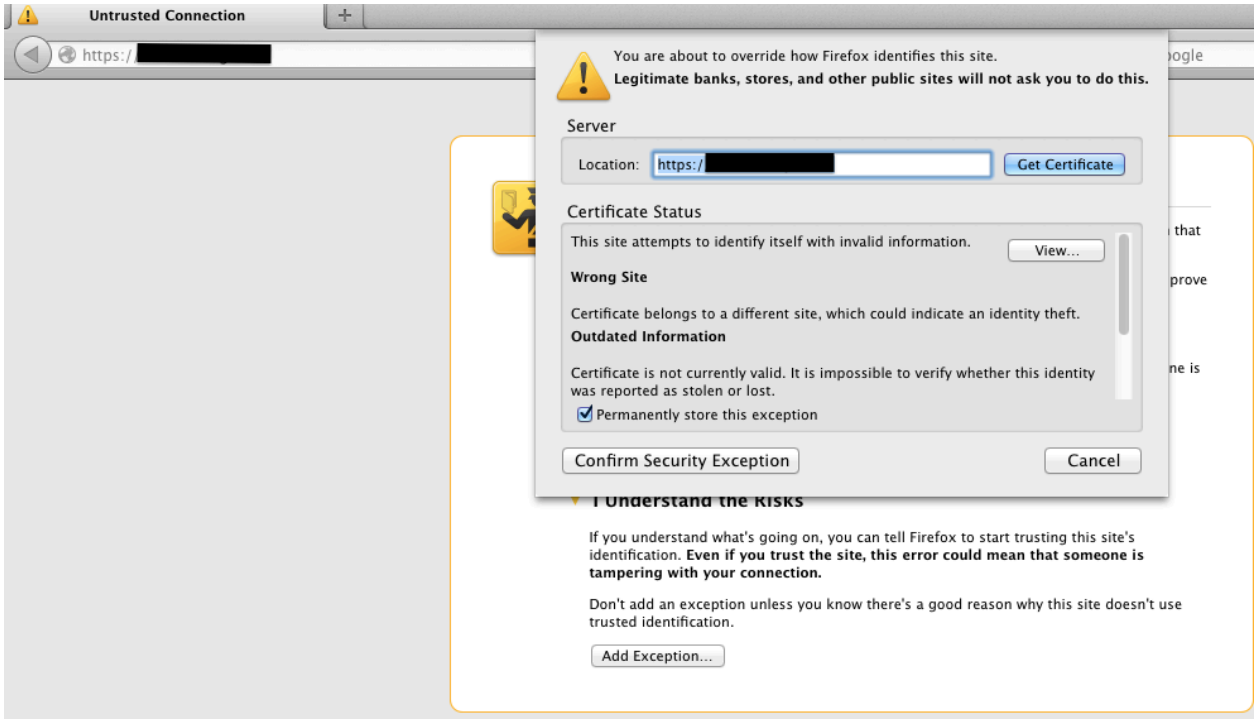
Khi người dùng đã chấp nhận chứng chỉ thì chứng chỉ sẽ được tính là hợp lệ và hiển thị màu xanh.

Đối với trình duyệt FireFox:

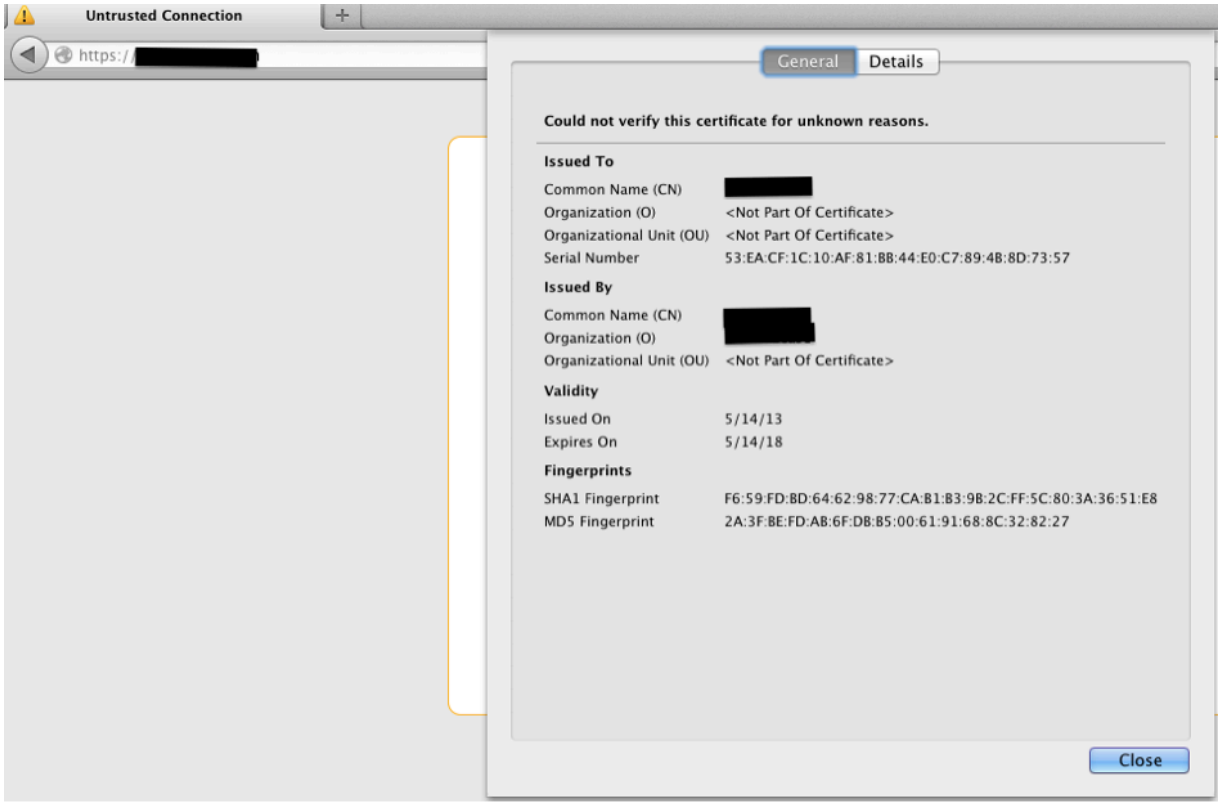
Tương tự trình duyệt Chrome, người dùng chọn "I Understand the Risk" -> "Add Exception...".



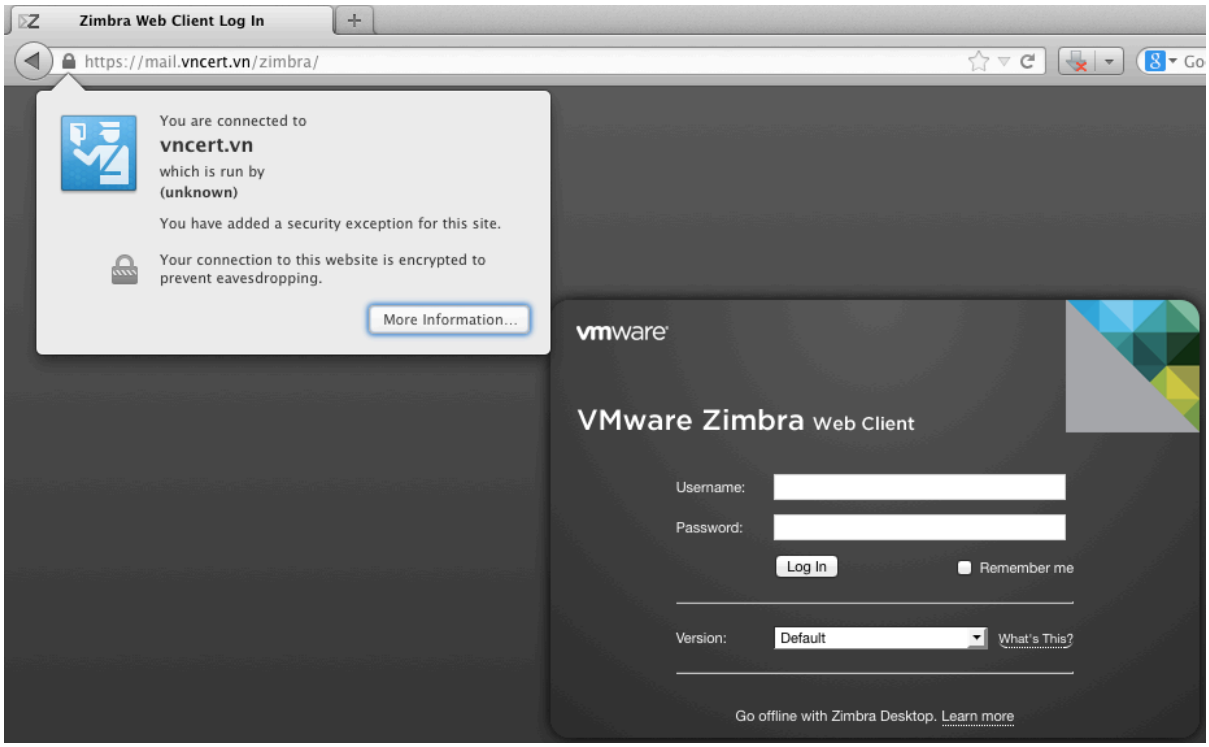
Một bảng thông tin về chứng chỉ sẽ được hiện lên, người dùng cần chọn "View" để kiểm tra thông tin chứng chỉ:



Sau khi chọn "View", thông tin về chứng chỉ sẽ được hiện ra. Người dùng so sánh mã băm lấy từ quản trị hệ thống với mã băm của chứng chỉ. Nếu hai giá trị này trùng nhau thì chứng chỉ là hợp lệ, còn không thì chứng chỉ bị giả mạo hoặc đã bị thay đổi. Người dùng cần dừng truy cập để tránh bị đánh cắp thông tin đăng nhập và nội dung email.

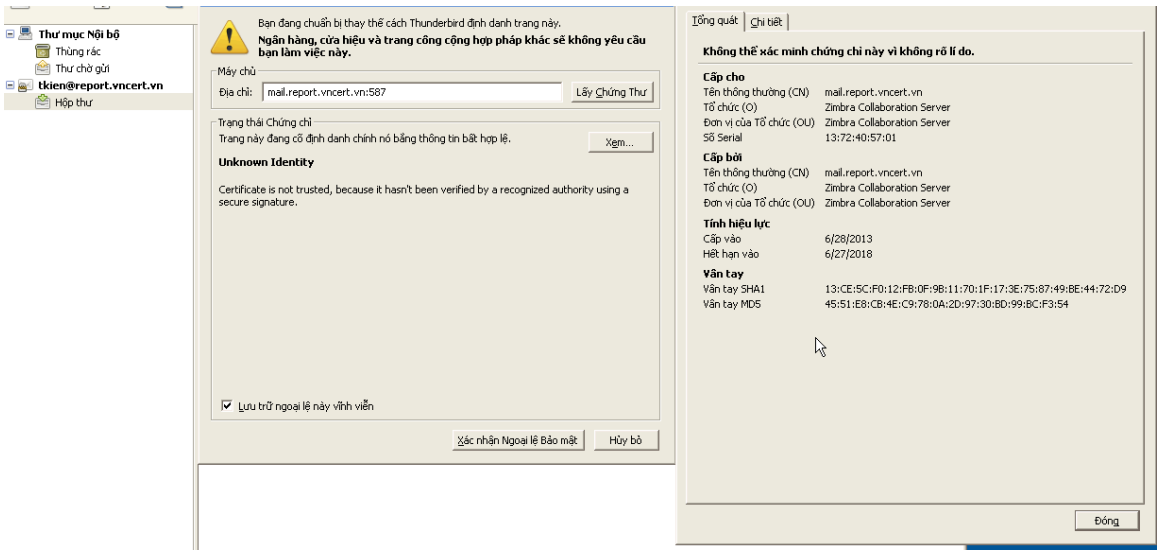


Trong trường hợp các giá trị là trùng nhau thì người dùng chọn "Close" và xác nhận "Confirm Security Exception". Chứng chỉ số sẽ được cài đặt vào hệ thống và dấu hiệu gạch đỏ sẽ mất:



Đối với các ứng dụng Email client cũng tương tự. Khi có một chứng chỉ mới từ phía server các ứng dụng sẽ hỏi người dùng có sử dụng chứng chỉ đó không. Trong trường hợp so sánh giá trị băm không trùng nhau, người dùng cần xác nhận lại với quản trị hệ thống về vấn đề có thay đổi chứng chỉ số hay không. Nếu không có thay đổi gì từ phía máy chủ thì chắc chắn là đường truyền đã bị nghe lén hoặc giả mạo chứng chỉ số. Người dùng cần phải dừng truy cập ngay lập tức và không xác nhận chứng chỉ số đó.

Dưới đây là ví dụ xác thực chứng chỉ trên Thunderbird(tương tự FireFox):

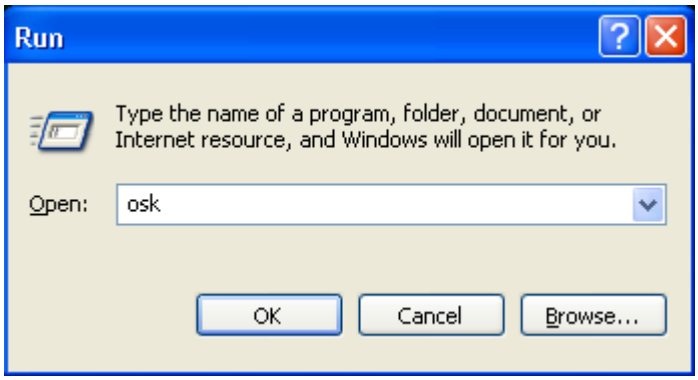


Phụ lục D: Hướng dẫn bật bàn phím ảo trên các hệ điều hành

D.1 Microsoft Windows

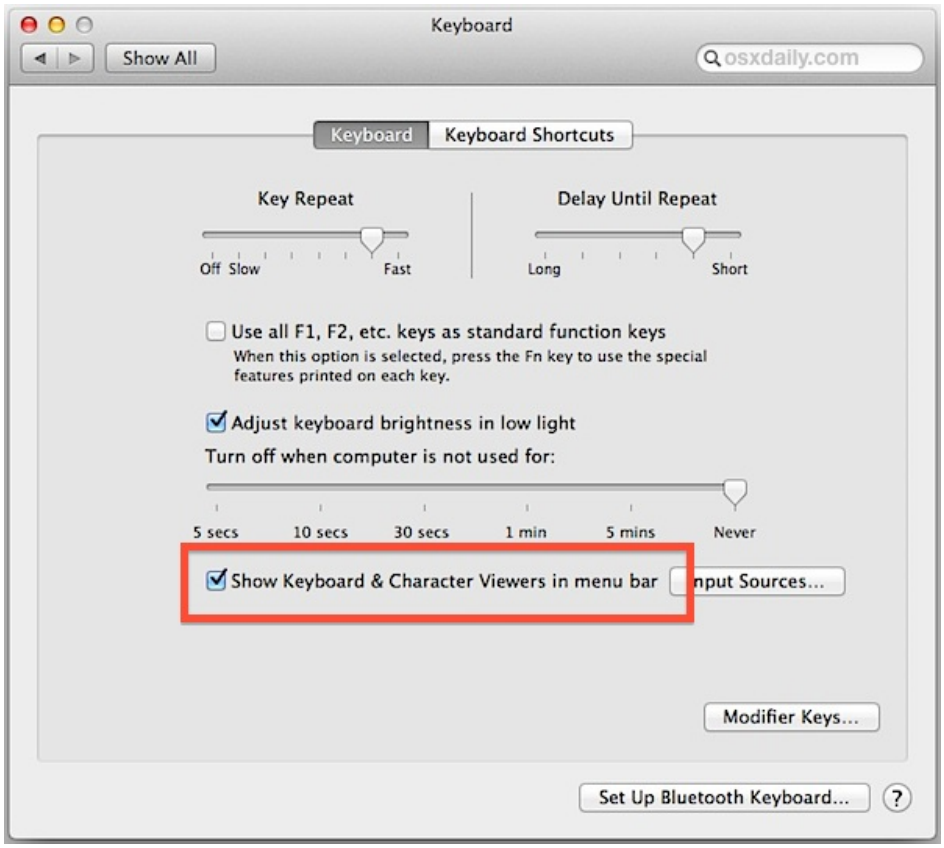
- Cách 1: Dùng phím Start -> All Programs -> Accessories -> Accessibility và chọn On-Screen Keyboard.

- Cách 2: Dùng phím Start -> Run và gõ "osk"



D.2 Mac OS X

- Mở System Preferences để vào Keyboard, tích vào ô lựa chọn "Show keyboard & Character Viewier in menu bar"



- Ngoài màn hình nền, mở thanh công cụ Keyboard và chọn "Show Keyboard Viewer"

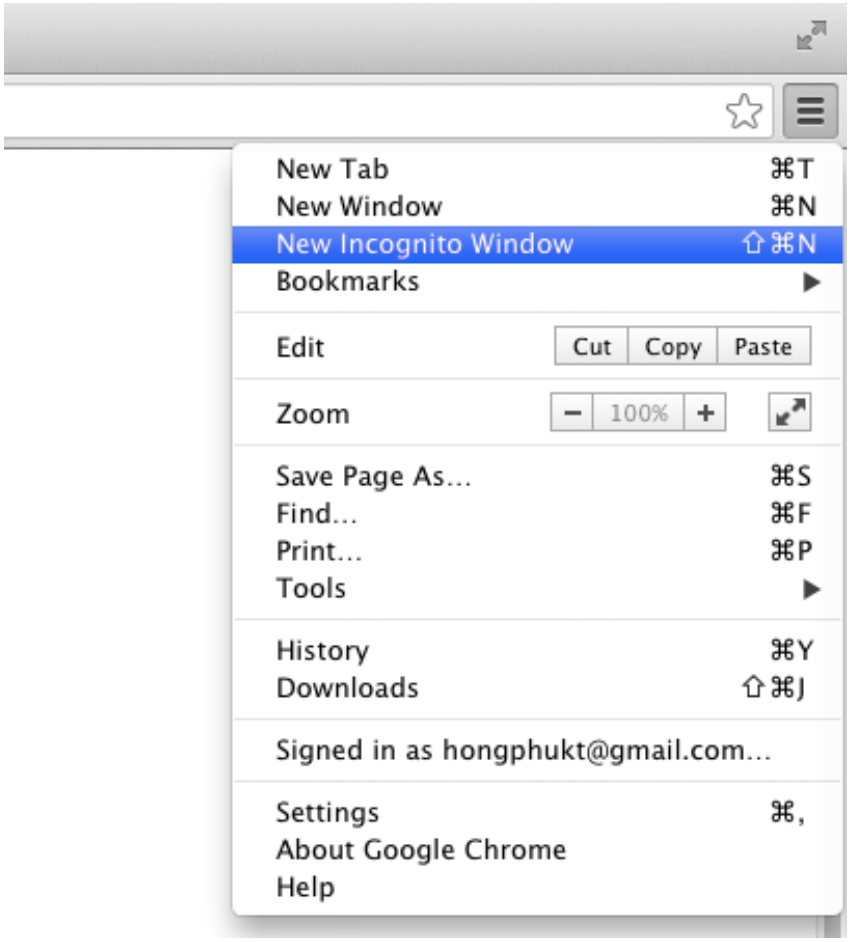
Sẽ hiện ra bàn phím ảo như sau:

Phụ lục E: Hướng dẫn sử dụng trình duyệt ở chế độ private

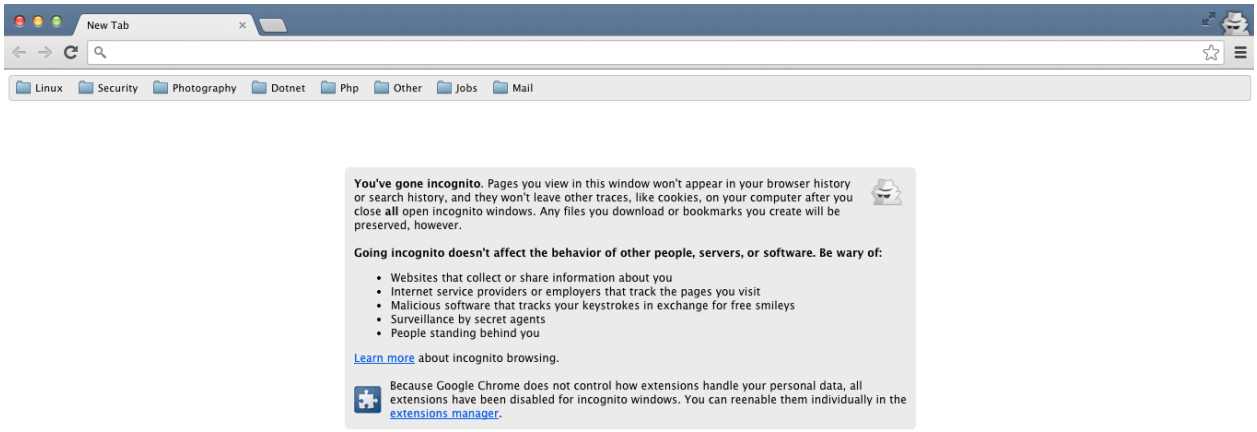
Các trình duyệt cung cấp sẵn chế độ private cho người sử dụng. Khi dùng ở chế độ này các history, cache sẽ được xoá ngay khi người dùng thoát ra. Việc truy cập thư điện tử tại các máy tính công cộng hay không phải máy tính cá nhân được thực hiện bằng trình duyệt web. Dưới đây sẽ là hướng đẫn cách sử dụng chế độ private browser cho người dùng:

E.1 Trình duyệt Chrome:

Người dùng nhấn vào biểu tượng "Customize and control Google Chrome" ở phía trên bên phải trình duyệt và lựa chọn "New Incognito Windows"(Mở cửa sổ ẩn danh mới):

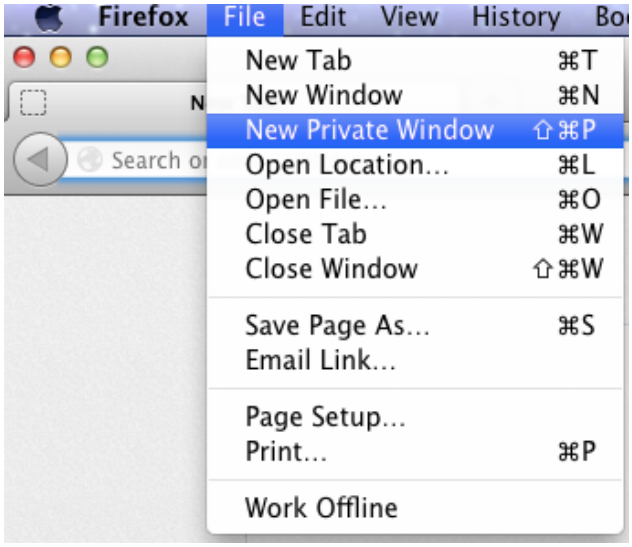


Hoặc người dùng có thể nhấn tổ hợp phím " Command + Shift + N" trên MacOS hoặc "Ctrl + Shift + N" trên Windows. Trình duyệt ẩn danh sẽ được hiển thị và người dùng có thể thao tác thoải mái ở đây mà không lo bị lưu trữ lịch sử truy cập:

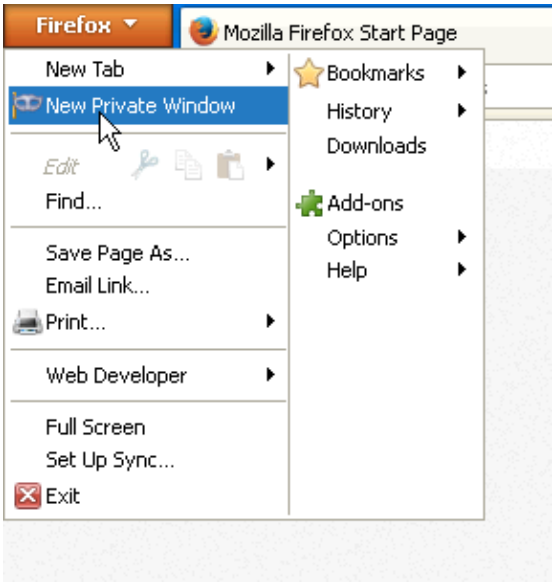


E.2 Trình duyệt FireFox:

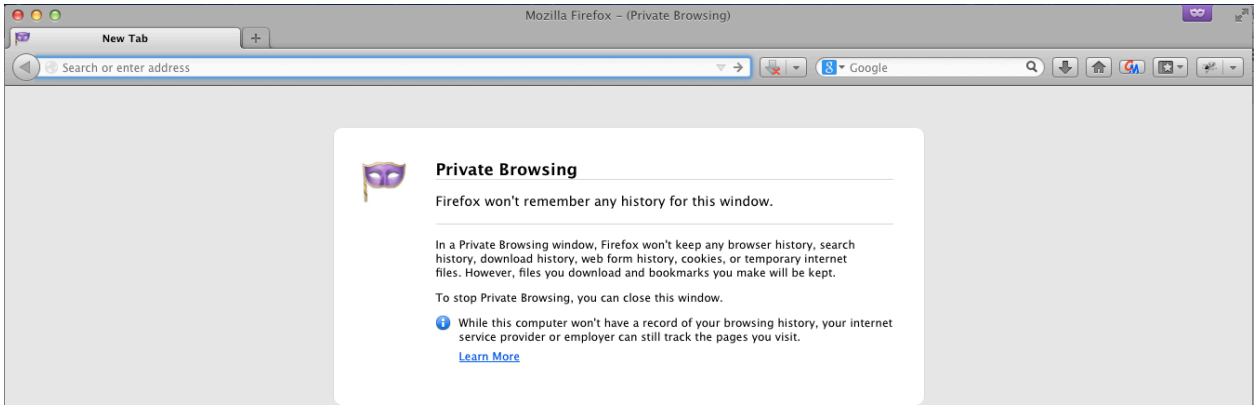
Người dùng mở FireFox và lựa chọn "File -> New Private Windows" hoặc "Command + Shift + P" với MacOS:



Và lựa chọn "Firefox -> New Private Window" hoặc "Ctrl + Shift + P" đối với Windows.

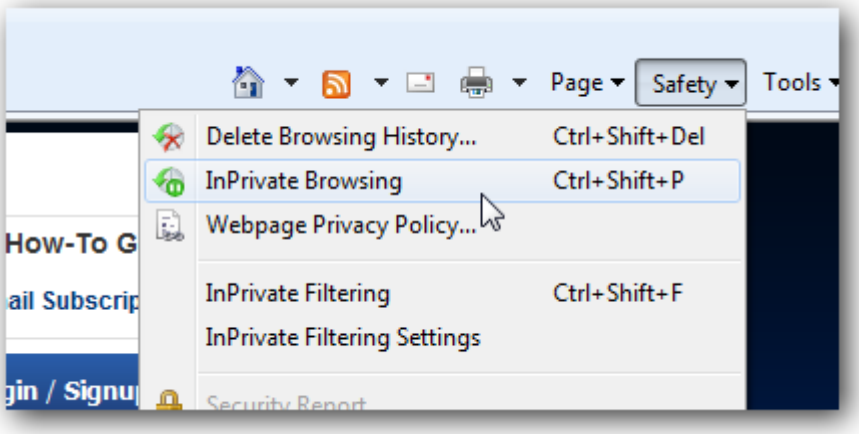


Khi đó trình duyệt private browsing của Firefox sẽ được hiển thị:



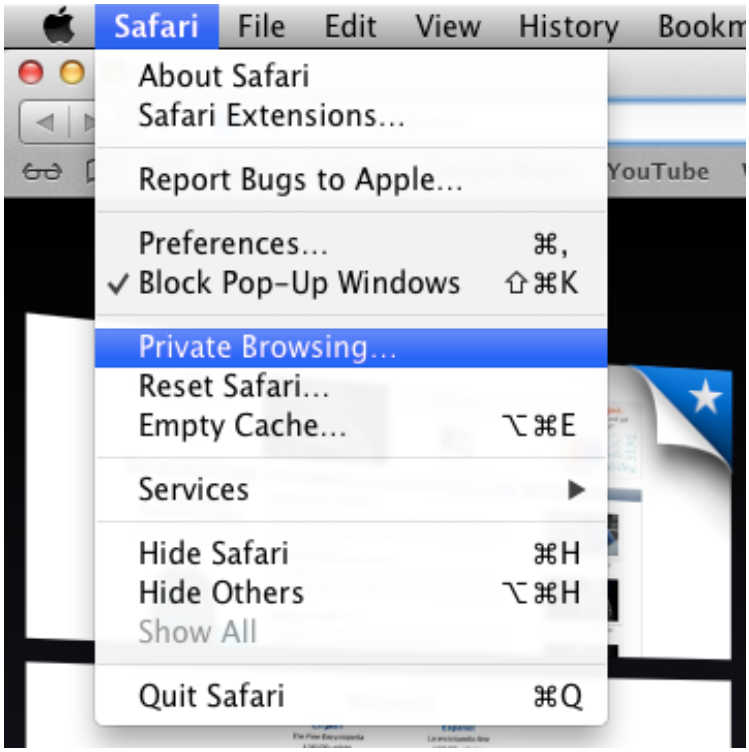
E.3 Trình duyệt Internet Explorer:

Người dùng IE có thể mở trình duyệt private bằng cách chọn "Safety -> InPrivate Browsing" hoặc tổ hợp phím "Ctrl + Shift + P":



E.4 Trình duyệt Safari:

Người dùng khởi động Private Browsing bằng cách lựa chọn "Safari -> Private Browsing":



Như vậy người dùng đã có thể sử dụng trình duyệt tại các máy tính công cộng mà không lo bị lưu trữ thông tin truy cập trên history hoặc cache của trình duyệt.