PHƯƠNG PHÁP CHUNG VƯỢT TƯỜNG LỬA CỦA CỘNG SẢN HANOI & LƯỚT WEB AN TOÀN

Lê Tùng Châu

Bypass Fire Wall

Trước hết, để đạt được cách vượt tường lửa (bypass firewall) của tà quyền hanoi ngăn công dân trong nước không vào được các trang mạng đối lập ở hải ngoại, hay ngay trong nước như bauxite Việt Nam, các Blog bất đồng chính kiến (Dissident) khác, chúng ta phải tuyệt đối không lướt web (surf web) –với các duyệt trình web thông dụng như IE hay Firefox- trong trạng thái mặc định, nghĩa là đi trực tiếp qua cổng proxy của hanoi.
Như thế chúng ta sẽ có nguy cơ lọt vào tầm kiểm soát của bọn chúng (trên nguyên tắc, chúng có thể "mò" ra ta với các chi tiết nhân thân của thuê bao Internet ta đang dùng nếu chúng muốn).

Mà ta phải surf web qua một số trang Proxy trung gian, hay sửa đổi trình duyệt web theo cách truy cập thông qua các proxy miễn phí (luôn có dầy dẫy trên Net).

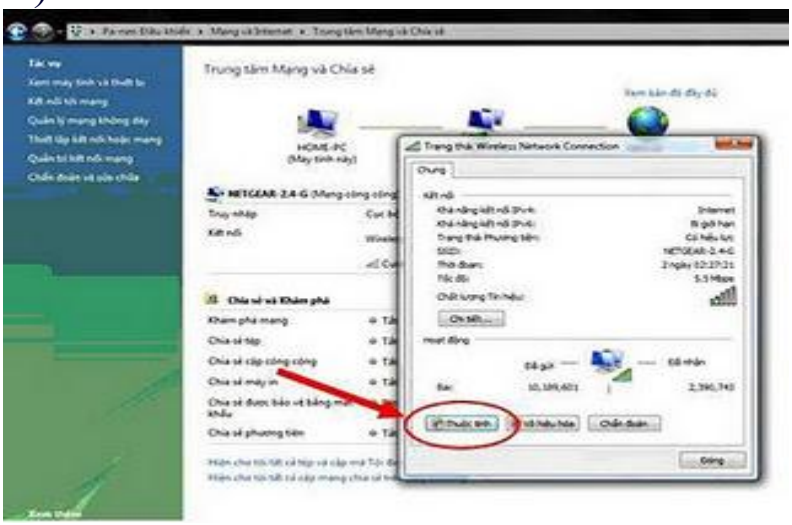
Thủ Tục quan trọng : Trước khi vào phần chính, tôi xin các bạn đổi hẳn (permanently) DNS (Domain Name Service) như sau :

Có nhiều cách khác nhau, một cách là:
Bạn vào "Control panel" ("Pa-nen Điều khiển")

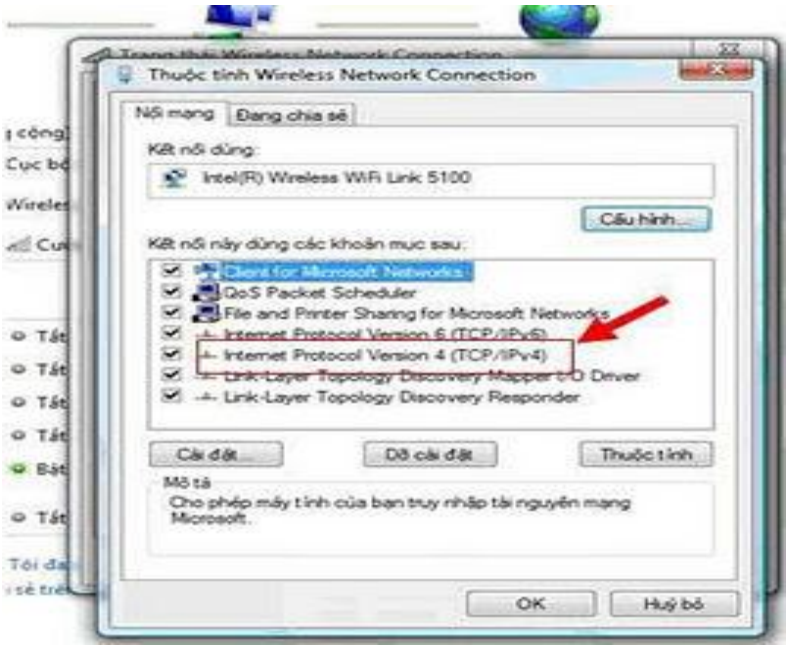
Chọn "Network status" ("Xem tác vụ và trạng thái mạng")

Bấm vào "Current network" hoặc "Network status" ("Xem trạng thái")

Sau khi bấm vào đó, sẽ có cửa sổ hiện ra, chọn "Properties” (“Thuộc tính”)

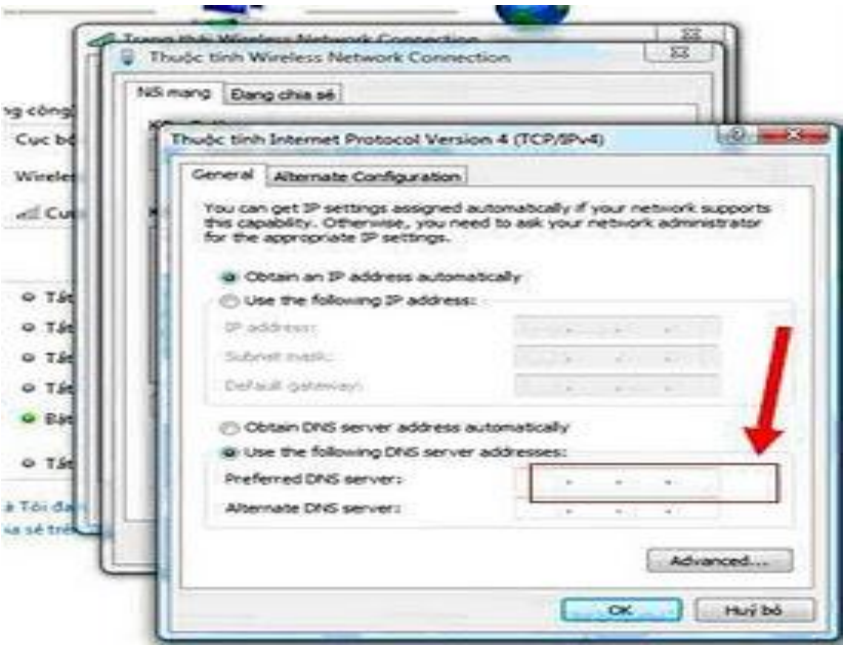


Tìm "Internet protocol version 4” và bấm vào đó



Bấm vào "Properties"("Thuộc tính"), tới đây bạn sẽ thấy một cửa sổ khác hiện ra

Chọn "Use the following DNS server addresses"



Sau đó gõ vào DNS server mà mình muốn. Trong trường hợp này bạn sử dụng của Google (8 8 8 8), hàng dưới "Alternate DNS Server" là 8 8 4 4.

Sau khi chọn DNS server rồi, Internet browser của bạn sẽ sử dụng DNS server mới này. Với cách giản dị này, bạn sẽ dùng được Facebook và những trang mạng khác bị chặn.

Tiếp theo, chúng ta còn cẩn thận thao tác một số bước sau để dùng Proxy khi surf web :

Hoặc Qua trang Proxy Server trung gian của các quốc gia tự do phương Tây

Theo kinh nghiệm của tôi, bạn có thể dùng 1 trong các trang sau :

1 / http://anonymouse.org/anonwww.html
2 / http://freeproxyserver.net/

3 / http://www.zend2.com
4 / http://www.anonymous-browsing.info/
5 / http://www.9mah.info/
6 / http://www.browser9.com/

Cách thức : Ở mỗi trang dạng này, bạn sẽ tìm thấy 1 "surf box" (kế bên có chữ GO hoặc SURF), ta copy link của trang ta cần đến rồi paste vào box (**1**/), sau đó click GO (**2**/) để load trang ta cần, ví dụ như sau :

Từ đây, bạn đã lướt web thông qua trang chủ http://freeproxyserver.net/ và mọi theo dõi của bọn an ninh mạng với bạn là vô hiệu. Có một số Proxy Server online như vầy cho

phép ta "mượn " đường để vào Blog hay mở email, có cái không cho, chỉ cho duyệt web thôi, ta hãy dùng thử sẽ có kinh nghiệm. Nhưng nếu dùng được cách này thì bọn cháu ngoan cộng sản bó tay để hack mail box hay Blog của bạn.

Hoặc Set lại duyệt trình web theo cách truy cập thông qua các proxy miễn phí :

A / Nơi lấy free proxy number : một trong các trang sau :

http://www.samair.ru/proxy/type-01.htm

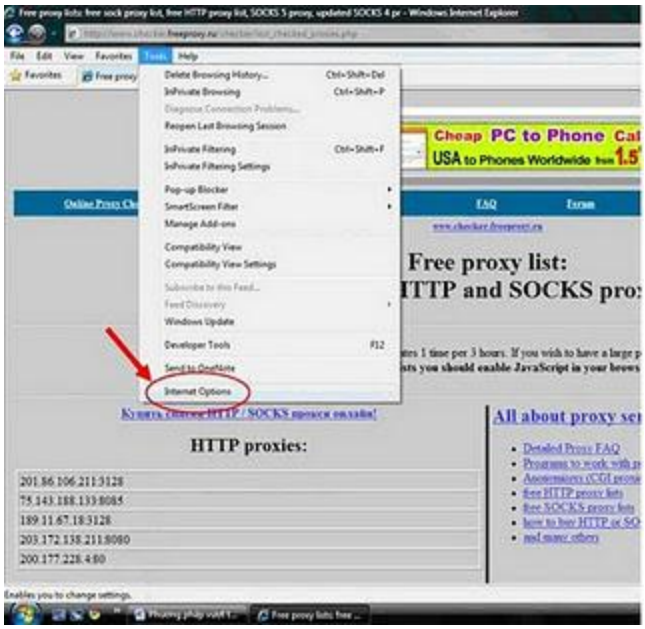
hoặc : http://www.proxylist.net/list/us/0/1

Kinh nghiệm của tôi: các proxy number của Nam Hàn (South Korea), Ấn Độ, Indonesia, Taiwan, Mexico, Brazil, Colombia, Mỹ, Canada, Netherlands là nhanh.

B / Set proxy cho duyệt trình web :

Bạn để ý thấy 1 số proxy luôn có kèm theo số Port, ta sẽ dùng 2 số đó để set nơi IE hay Firefox như sau :

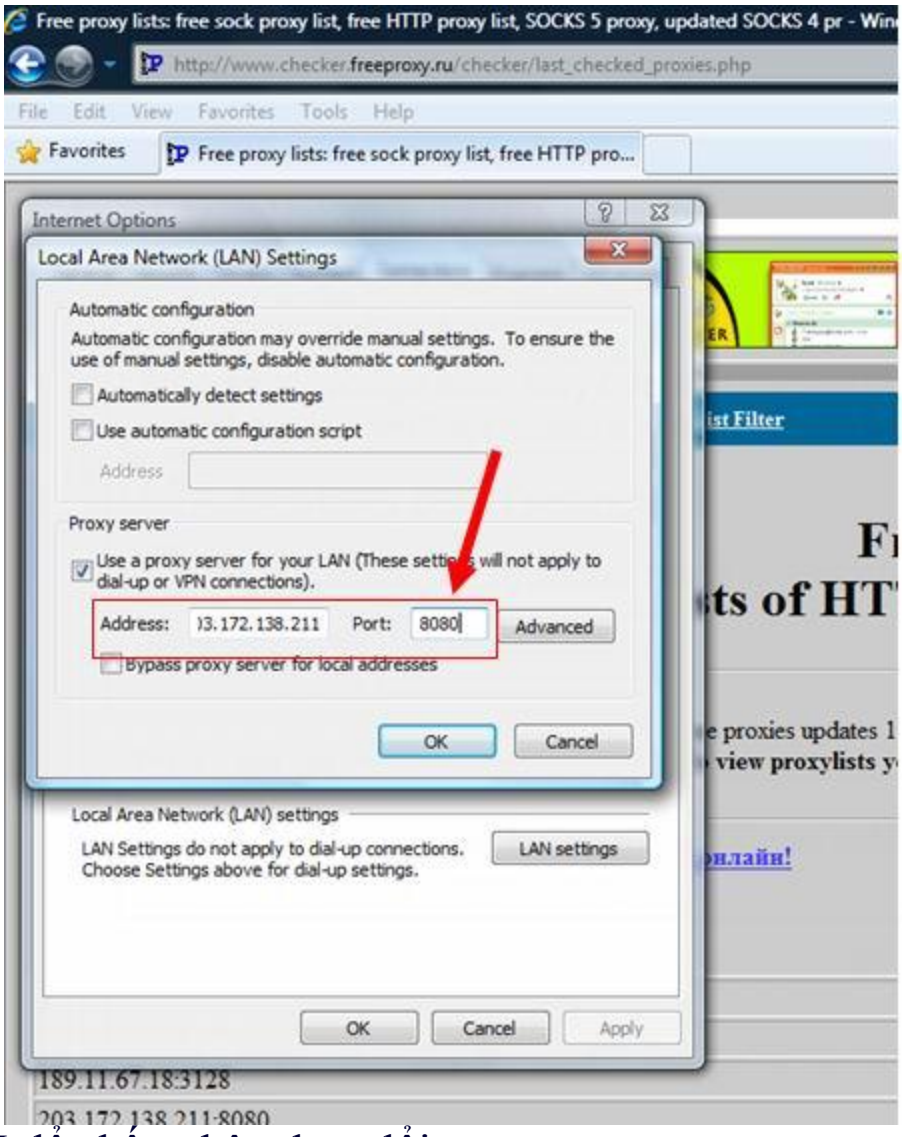
Với IE (Internet Explorer)
Chọn "Tools", sau đó "Internet options"



Tới đây có cửa sổ hiện ra. Chọn “Connections”, và sau đó “LAN settings”

Chọn "Use a proxy server for your LAN"

Copy và Paste Proxy number vào box "Address" và Copy và Paste số Port (4 số) tương ứng vào box "Port"



Click OK để chấp nhận thay đổi.

Với Firefox :

Tools --> Options --> Advanced --> Settings --> chọn "Manual Proxy confirguration" rồi copy và paste số proxy chọn được vào box "HTTP Proxy" và copy và paste số Port tương ứng vào box "Port". Click OK để chấp nhận thay đổi.

Để biết có thành công không (tức là số proxy ta vừa chọn có hiệu

lực không), bạn thử mở Google, nếu số proxy ta vừa chọn của nước nào thì sẽ hiển thị Google của nước đó. Đó là thành công. Nếu không được (không hiển thị, hoặc lâu quá, châm quá), bạn hãy chọn 1 số proxy khác. Dùng nhều sẽ có kinh nghiệm và thao tác thay đổi proxy diễn ra chừng vài chục giây là cùng.

Từ đây bạn cứ sử dụng Internet Explorer hoặc Firefox bình thường, nhưng lần này bạn sẽ đi qua Proxy mà mình đã lựa chọn thay vì Internet server của Việt Nam.
Khi dùng Proxy, bạn có thể sẽ thấy tốc độ Internet chậm hơn, tùy số Proxy nơi quốc gia nào, và tùy vào thời điểm ta online nữa.!
Hơn nữa, đôi khi có Proxy không hoạt động. Có thể nó đã "chết". Trong trường hợp đó bạn phải thay một Proxy khác (cũng từ các trang đã cho ở trên)

Như trên đã trình bày thì việc Bypass Firewall coi như xong. Ý nghĩa của việc Set lại proxy server cho duyệt trình web như vầy khác với việc dùng **Proxy Server trung gian** (để coi web như nói ở mục trên) là ở chỗ, ta có thể gởi, nhận mail hay sign in Blog một cách an toàn, bảo mật chứ không riêng gì coi tin tức trên các web bị chận tường lửa! Điểm bất tiện của cách này là cứ thỉnh thoảng vài ngày ta phải tìm số proxy mới để thay thế nếu số proxy đang dùng bị "chết" (time out).

LƯỚT WEB AN TOÀN (hay Tàng Hình trên Mạng)

Sau đây chúng ta hãy gắng tí nữa để có thể "tàng hình" khi online : (tài liệu dưới đây rất quan trọng và hữu hiệu, trích từ PC World, 5/2006 (http://www.pcworld.com.vn/articles/cong-nghe/ung-

dung/2006/05/1189014/bao-mat-cong-445-trong-windows-2000-xp-2003/). Tôi có hiệu chỉnh một ít và thêm hình minh họa.

Bảo mật cổng 445 trong Windows

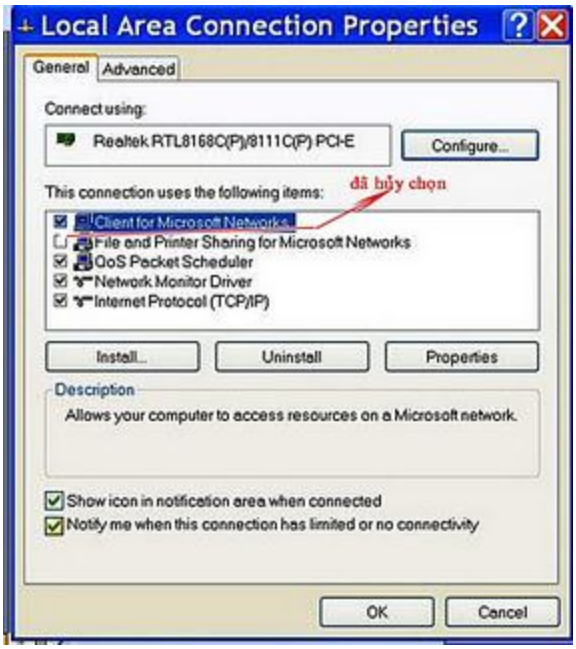
Trên các hệ thống Windows 2000, XP và Windows Server 2003 có một số cổng mới được sử dụng, trong số đó, cổng (port) 445 TCP dùng cho dịch vụ SMB truyền qua TCP.

SMB (Server Message Block) được sử dụng cho mục đích chia sẻ file. Trên các hệ thống Windows NT cũ nó vận hành với NetBT (NetBIOS over TCP/IP), sử dụng các port thông dụng như 137, 138 (UDP) và 139 (TCP). Trên các hệ thống Windows 2000/XP/2003, Microsoft hỗ trợ khả năng vận hành trực tiếp SMB qua TCP/IP (port 445), không cần qua NetBT.

NetBIOS cho phép thực hiện đơn giản việc chia sẻ file qua mạng nội bộ (LAN), tuy nhiên đó lại là mối nguy hiểm tiềm tàng khi hệ thống kết nối WAN hay Internet. Tất cả thông tin về mạng (như tên miền) và tài khoản truy cập mạng nội bộ của bạn đều có thể bị thu thập.

Cấm NetBT

Trên Windows 2000/XP/2003 tiến hành cấm NetBT như sau: (Nhấn phải chuột vào) Local Area Connection tại Task Bar bên dưới màn hình, chọn Status, chọn thẻ General, sau đó chọn Properties. Trước hết hủy chọn nơi “File and Printer Sharing for Mocrosoft Networks”



tiếp tục click vào Internet Protocol (TCP/IP) kế đó click Properties; rồi click vào Advanced và chọn tab WINS. Tại đây bạn chọn Disable NetBIOS over TCP/IP, click OK để chấp nhận thay đổi, thay đổi có hiệu lực ngay, không cần phải khởi động lại hệ thống.

Lưu ý, các máy tính chạy HĐH trước Windows 2000 sẽ không thể định vị, tìm kiếm hoặc thiết lập kết nối chia sẻ file và in ấn đến các máy tính Windows 2000/XP/2003 khi NetBT bị cấm.

Cấm cổng 445 (*để tham khảo thêm*)

Theo báo cáo của SANS.Org, port này có tần suất bị tấn công cao nhất (thông tin chi tiết tại http://isc.sans.org/port_details.php?port=445). Port 445 có thể cấm theo các bước sau:

1. Mở trình Registry Editor: vào Run, gõ regedit.

2. Tìm đến khóa HKLM\System\CurrentControlSet\Services\NetBT\Parameters

3. Trong cửa sổ bên phải, chọn TransportBindName.

4. Nhấn đúp chuột (hay gõ Enter) và xóa giá trị của biến này (khung Value data được để trống).

5. Đóng Registry editor

6. Khởi động lại máy tính

Sau khi khởi động và đăng nhập vào máy tính, tại Run, gõ lệnh cmd và nhập lệnh sau:

netstat -an

Bạn sẽ thấy máy tính không còn "lắng nghe" ở port 445.

Khi nào Windows 2000/XP/2003 dùng port 445 và khi nào dùng 139?

Để đơn giản, tôi dùng thuật ngữ "client" để chỉ máy tính truy xuất các nguồn tài nguyên mạng như ổ đĩa và các file được chia sẻ tại "server" - máy tính có nguồn tài nguyên.

Nếu server có NetBT được bật, nó sẽ lắng nghe trên port 137, 138 (UDP) và trên port 139, 445 (TCP). Nếu NetBT bị cấm, server chỉ lắng nghe trên port 445 (TCP).

Nếu client có NetBT được bật, nó sẽ luôn thử kết nối đến server đồng thời tại port 139 và 445. Nếu nhận được phản hồi từ port 445, nó sẽ gửi phản hồi đến port 139 và tiếp tục phiên giao tiếp SMB chỉ với port 445. Nếu không nhận được phản hồi từ port 445, nó sẽ tiếp tục giao tiếp SMB chỉ với port 139, khi nhận được thông tin phản hồi từ port này. Nếu không nhận được bất cứ phản hồi nào từ 2 port trên, kết nối sẽ kết thúc.

Khi client có NetBT bị cấm, nó sẽ luôn kết nối đến server tại port 445. Nếu server trả lời trên port 445, kết nối sẽ được thiết lập. Nếu không nhận được trả lời, kết nối kết thúc.

(**Ho Viet Ha, Network Information Security Vietnam**)

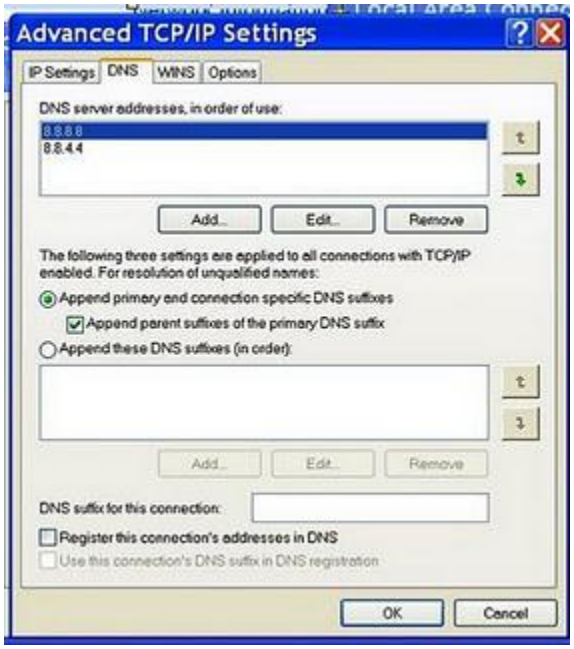
* * * * * *

Cũng trong số PC World này còn bổ sung thêm cho biện pháp **Disable Netbios Over TCP IP** trong bài **Cài đặt, cấu hình, quản trị ISA Server 2004 Firewall** (http://www.pcworld.com.vn/articles/cong-nghe/ung-dung/2006/05/1189012/cai-dat-cau-hinh-quan-tri-isa-server-2004-

firewall/) như sau (trích) :

["……..Nhằm bảo đảm an toàn cho hệ thống và firewall, trên giao tiếp mạng Outside chọn Disable Netbios Over TCP IP, hủy chọn "Register this connections address in DNS" và "Enable LMHOST lookup" như các hình sau:

Và :



Lưu ý: Chức năng Disable NetBIOS over TCP/IP làm cho máy tính trở nên "vô hình" trên mạng, các phần mềm quét lỗi hệ thống như Retina, Nmap sẽ không tìm thấy tên của máy tính, hạn chế trường hợp dò tìm password của những tài khoản theo cơ chế brute force. Các máy chủ giao tiếp với Internet như firewall thường chọn chức năng này, tuy nhiên đối với các máy tính trên mạng nội bộ chúng ta không nên sử dụng vì sẽ ngăn các máy tính khác truy cập vào tài nguyên chia sẻ trên máy như Printer, Folder Share. [Một số ứng dụng bảo mật (như PC Security) khi cài đặt sẽ mặc định chọn Disable NetBIOS over TCP/IP] -hết trích-

* * *

Một "lỗ hổng" thông thường dễ mắc phải là chúng ta hay tạo nick cho một Mail Account theo các chi tiết về nhân thân của mình, như tên họ ngày tháng năm sinh v.v... Tôi xin góp ý các bạn, tuyệt đối không nên! (Và càng không nên dùng Yahoo Mail cho những việc cần độ bảo mật, an ninh cao. Hãy tạo Mail Account nơi aol.com, gmail.com hay hotmail cũng được, những nơi này bạn được bảo mật gần như tuyệt đối) Ta hãy dùng một tên riêng nào (ví dụ như tên các cầu thủ soccer, tên nhạc sĩ hay vĩ nhân nào ta thích...) không hề liên quan đến bản thân mình, đa số bọn an ninh VC thường mò ra "nạn nhân"*của chúng từ Yahoo Mail nào đã "thực thà" tạo nick name theo đúng tên mình (thậm chí có cả ngày tháng năm sinh kèm theo nữa!!! Các bạn chú ý điều này, tuy nhỏ nhưng quan trọng. Với những email quan trọng cần bảo mật, ta nên xóa (thường mặc định được save vào Sent Folder) ngay sau khi đã gởi thành công. Và thao tác những việc gì cần thiết trên Mail Box thật nhanh xong sign out ngay, không nên mở "tô hô" lâu quá không cần thiết. Dĩ nhiên đừng quên thay đổi Password mỗi 1tuần/ hoặc 2 tuần*

Tổng quát như trên là những biện pháp không thể thiếu khi một cá nhân online tại nhà hay café Net hay một nơi lạ nào khác. Ta phải chịu khó thực hiện các thao tác này thật nhanh gọn để có thể yên tâm làm việc riêng tư trên Mạng mà không sợ bị rình rập hay trộm cắp những riêng tư nữa.

Sau chót, nếu bất cứ lúc nào, nơi nào, bạn muốn xóa hết dấu vết mình đã làm gì, truy cập gì trên PC, bạn nhất thiết phải delete history (IE hay Firefox) trước khi rời máy.

Mong các bạn thực nghiệm và có bất cứ thắc mắc phản hồi xin cứ comment cho tôi biết, sẽ kịp thời support các bạn trong khả năng nhanh nhất có thể.

Chào thân ái!

LTC
(viết theo kinh nghiệm cá nhân, và có tham khảo các nơi như http://viettan.org/spip.php?rubrique427, PC World tháng 5/2006)

Nguồn: http://letungchau.blogspot.com/2010/07/phuong-phap-chung-vuot-tuong-lua-cua.html