

Email bị tin tặc tấn công:

Đây là sự thật, tất cả những vị sử dụng email để chuyển tải những tin tức quan trọng cần chú ý. Tất cả quý vị thường xuyên sử dụng email, dù có làm việc cộng đồng hay không, quý vị có thể là mục tiêu tấn công của tặc Tàu và tin tặc Việt Cộng. Cách tốt nhất, quý vị phòng chống tin tặc để bảo vệ sự riêng tư của mình trước khi quá trễ. Có thể công việc làm ăn của quý vị bị chúng phát giác, có thể những thảo luận cần giữ kín của quý vị bị tiết lộ, có thể chi tiết ngân hàng, chi tiết chuyển tiền bị tin tặc biết được, v.v... Những biện pháp bảo vệ này, chỉ mất công chút ít nhưng không mất tiền mua, dù không đoan chắc có hiệu quả 100% nhưng ít nhất cũng là một rào cản làm nản lòng tin tặc.

Trần Đông, MSc.

Cuối tuần trước, đó là lần thứ hai email của tôi bị tin tặc VC tấn công trong vòng một tháng. Và cuối tuần vừa qua, lần thứ hai trong vòng một tuần chúng tấn công email của tôi. Lần đầu tiên, cuối tháng trước, chúng vào email của tôi và cho vào một lệnh để chuyển tất cả email của tôi tới một địa chỉ khác. Lần này, chúng phá hoại nhiều hơn, chúng thay đổi mật mã vào email của tôi, đồng thời cả hai email, chúng đều cho vào một lệnh để chuyển mail đến một địa chỉ email khác. Sau khi phát giác, tôi kiểm soát lại phần settings của email và quả thật, chúng đã gài vào lệnh chuyển email tôi tới một chỗ khác. Khôn ngoan hơn, chúng không chỉ gài lệnh chuyển, nghĩa là email vẫn vào hộp thư của tôi, nhưng đồng thời chúng cũng nhận được một bản để xem. Lần thứ ba giống như lần thứ hai, chúng đổi mật mã, cài lệnh chuyển email đến một địa chỉ email khác.

Tôi có thể chắc chắn đây là tin tặc Việt Cộng. Thứ nhất, lệnh chuyển email được cài cho một người có tên theo mẫu tự Việt ngữ. Và vì một vài yếu tố khác không tiện tiết lộ ra đây, nên tôi có thể đoan chắc rằng đây là tin tặc Việt Cộng, không phải là hackers người nước ngoài.

Cuối tuần đi họp, được biết một số anh chị em hoạt động trong BCH CĐ cũng bị tin tặc phá. Chúng viết email thay cho anh bạn có tên abcdef@hotmail.com và chuyển email đến những người có tên trong Contact list của abcdef với nội dung bậy để khuấy rối. Điều đó cho thấy mục tiêu tấn công là những vị trong Ban Chấp hành Cộng đồng Người Việt các nơi, các vị làm việc cho truyền thông Việt Ngữ, các vị giữ các chức vụ quan trọng trong các Hội đoàn Đoàn thể, Đảng phái chính trị, kể cả các doanh nhân khá tiếng tăm đều có thể là mục tiêu của tin tặc VC.

Tại sao tin tặc VC tấn công chúng ta? Chúng tấn công nhằm mục đích gì?

Theo tôi thấy chúng ta có thể phân tích mục tiêu của chúng như sau:

Mục đích chính trị:

- Chúng muốn tìm kiếm những tin tức liên quan đến các tổ chức đấu tranh trong nước và tại hải ngoại. Đây là nhiệm vụ chủ yếu.
- Chúng muốn tìm kiếm những tin tức liên quan đến công ăn việc làm của những nhân vật hải ngoại. Nếu những nhân vật này có liên hệ đến những người trong nước, chúng cố tìm những chứng cứ để khi cần thiết chúng sẽ bắt chẹt chúng ta hoặc người trong nước để làm công cụ cho chúng.
- Chúng muốn khuấy rối và vô hiệu hóa hoạt động của các nhân vật và đoàn thể hải ngoại

Mục đích kiếm tiền:

Chúng ta không loại trừ trường hợp nếu chúng có thể dò tìm những dữ kiện để chúng có thể móc của chúng ta, chắc chắn chúng sẽ không bỏ qua. Thí dụ chi tiết trương mục, chi tiết vào trương mục trên mạng, nếu chúng biết được, chúng sẽ dễ dàng vào trương mục để chuyển tiền đi nơi mà chúng muốn.

Tất cả quý vị thường xuyên sử dụng email, dù có làm việc cộng đồng hay không, tất cả đều nên học hỏi cách thức phòng chống tin tặc để bảo vệ sự riêng tư của mình. Có thể công việc làm ăn của quý vị bị chúng phát giác, có thể những thảo luận cần giữ kín của quý vị bị tiết lộ, có thể chi tiết ngân hàng, chi tiết chuyển tiền bị tin tặc biết được, v.v... Những biện pháp bảo vệ này không đoan chắc có hiệu quả 100% nhưng ít nhất cũng là một rào cản có hiệu quả làm nản lòng tin tặc.

Dù phá hoại hay kiếm tiền hay tiêu khiển, hành động tin tặc đều bị lên án.

Tính chất phạm pháp của tin tặc VC:

Do bản chất luôn muốn chà đạp và coi thường luật pháp, tin tặc VC và nhóm lãnh đạo của tin tặc đã lộng hành trong nước, học hỏi những kinh nghiệm đó, nay chúng đi vào sử dụng ở nước ngoài. Gần đây tin tặc Trung cộng đã phá hoại nhiều nơi, hiện nay tin tặc VC ra sức phá hoại cộng đồng người Việt hải ngoại, hai sự kiện này cho thấy chắc chắn tin tặc VC có phối hợp hành động với tin tặc Trung cộng và minh chứng cho sự kiện nhà nước và lãnh đạo đảng CSVN là chủ hầu của CS Tàu, sẵn sàng công rấn cắn gà nhà để bảo vệ vị thế chủ nô bóc lột nhân dân tận xương tuỷ và đàn áp dân chủ tự do trong nước.

Hành động xâm nhập email cá nhân hay email tổ chức, hội đoàn, đoàn thể hải ngoại mang những ý nghĩa xấu xa và phạm pháp như sau:

- xâm nhập email là trắng trợn chà đạp và coi thường luật pháp của quốc gia sở tại;
- xâm nhập email là vi phạm đời tư và tự do thư tín của người khác;
- xâm nhập email là chủ trương phá rối sinh hoạt cộng đồng người Việt hải ngoại, xâm phạm sự an sinh của cộng đồng người Việt hải ngoại, lãnh vực mà chính phủ nước sở tại luôn coi trọng và bảo vệ;
- đây là một minh chứng cho thấy chủ trương của CSVN là luôn gây khó khăn cho Cộng đồng hải ngoại, luôn coi Cộng đồng hải ngoại là thù địch.

Quốc gia nơi chúng ta cư ngụ có Cảnh sát quốc nội và quốc tế, có cơ quan tình báo, có những cơ quan bảo vệ quyền riêng tư và an sinh xã hội, các Công ty cung cấp dịch vụ email luôn muốn tìm kiếm những tay tin tặc quấy rối để lôi cổ ra trước ánh sáng công lý, vì những lý do này tất cả chúng ta cần chung sức đưa những tên tin tặc VC ra truy tố trước pháp luật.

Làm sao tin tặc vào máy hay vào email của chúng ta được?

Tin tặc có những chương trình hay những lệnh để phá mật mã, phá mật mã được chúng sẽ vào máy được, vào email được. Những nơi này dù được bảo vệ nhưng không được chặt chẽ bằng hệ thống an toàn của ngân hàng nên việc tấn công ngân hàng rất khó, trong khi tấn công email hay vào máy điện toán cá nhân dễ dàng hơn nhiều.

Những máy điện toán để chạy ngày đêm là những nơi dễ cho tin tặc tấn công nhất. Chương trình phá mật mã có thể chạy liên tục cho đến khi phá được mới thôi. Những Windows không có mật mã hoặc không sử dụng chương trình diệt Virus và phòng chống xâm nhập là những Windows rất dễ bị tấn công. Những emails có mật mã đơn giản, hay cài "*nhớ mật mã*" để mỗi khi vào email không cần đánh máy mật mã, đó là những mục tiêu rất dễ phá và tạo điều kiện cho tin tặc tấn công dễ dàng.

A- Cần làm gì để bảo vệ máy và Email?

Đối với máy điện toán và Windows:

- 1- Tắt máy: Khi không sử dụng máy nên tắt máy. Vừa tiết kiệm điện, vừa tăng tuổi thọ của máy, vừa giảm bớt thời gian cho tin tặc tấn công.
- 2- Mật mã cho Windows: Windows phải có mật mã. Mỗi lần muốn vào chúng ta chịu khó đánh mật mã để vào. Mật mã phải được thay đổi ít nhất một tháng một lần.
- 3- Phòng chống bằng Windows: Windows phải có cài Firewall, cài chương trình diệt Virus cập nhật nhất (updated) và các loại phòng chống căn bản khác.
- 4- Cắt Internet: Khi không cần xài Internet rút dây nối Internet hay cắt đường nối Internet hay disable Internet. Khi cần sử dụng thì nối lại.
- 5- Sử dụng Hard Drive rời: những tài liệu quan trọng nên chứa vào Hard Drive rời, khi nào sử dụng chỉ cần gắn dây vào máy, khi không sử dụng thì rút dây ra. Hiện nay loại Hard Drive cầm tay rất nhỏ, bằng bàn tay, dày 10 ly, rất nhẹ, rất rẻ, sức chứa lại cao (80 Úc kim mua được 320Gb), chỉ cần một sợi dây USB gắn vào bất cứ máy điện toán nào. Tôi sử dụng 3 loại Hard Drive để chứa những tài liệu riêng nhau và chỉ gắn vào cần dùng. Trong máy không có tài liệu nào quan trọng cả.

B- Những bước cần thực hiện ngay khi đọc email này:

1- Đặt Username & Password (nếu đã có Unsername khi log-in xin xem mục)

- 1- In bản tin này ra một bản
- 2- Tắt email và application đang đọc này. Tắt tất cả các Windows đang mở, ngay cả Internet Explorer.

- 3- Lấy một tờ giấy và cây viết để ghi chú
- 4- Đặt mouse ngay Start, right click (click nút mouse bên tay phải), click Explore.
- 5- Ngay trên Windows đang mở là C:\Document and Settings..., right click vào My Computer, click Manage.
- 6- Click Local Users and Groups. Click Users. Một Windows mở ra.
 - a. Ở Username: đặt một tên (*ghi vào giấy. Cần ghi cho đúng*).
 - b. Ở Password: chọn một password ít nhất 8 mẫu tự. Password này sẽ phải thay đổi thường xuyên nên cần chọn Password sao cho dễ nhớ (*ghi vào giấy. Cần ghi cho đúng*).
 - c. Ở Confirm Password: đánh máy lại password.
 - d. Click Create. Click Close.
- 7- Click Start, click Log off. Chờ đến khi Windows logg off xong.
- 8- Click vào Icon có Username ở mục 6a bên trên. Đánh máy Password vào ô trống bên dưới. Click vào mũi tên ngang. Windows sẽ được log in.

CHÚ Ý: Nếu quý vị không tự tin sẽ làm được đúng nên nhờ người giúp vì nếu máy chưa có Username, quý vị ghi Username hay Password sai, quý vị sẽ không vào máy được.

II- Kiểm soát lại email & điều chỉnh Password:

Vì khuôn khổ hạn chế chúng tôi chỉ lấy thí dụ cho 3 loại email: Google, Yahoo và Hotmail mà thôi. Phần này quý vị sẽ kiểm soát lại email của mình để ghi lại những phần cần nhớ để phòng trường hợp password bị tin tặc thay đổi không thể log-in vào email được hoặc email thay đổi nhưng bị quên và không log-in được.

Trước khi thực hiện phần này quý vị cần có ít nhất là 2 emails để sử dụng. Một email dùng cho công chúng, email này được quảng cáo nhiều nơi, là mục tiêu của tin tặc. Và một hay hai emails khác để sử dụng trong trường hợp cần lấy lại password hay những chuyển những tin tức quan trọng.

GOOGLE	YAHOO	HOTMAIL
1- click Settings. 2- click General. In ra giấy để lưu. 3- click Accounts and Imports. Click Google Account Settings. Click Change password recovery settings. Đánh máy password vào. Click Verify. Một Windows mới mở ra. 4- Xem phần email. Phần này ghi tên email của quý vị khi cần lấy password lại. Cần ghi 2 hay 3 emails vào nơi này. Xong, click save. 5- Click vào Change Password để đổi Password. Đánh máy Password mới, đánh máy Password mới một lần nữa để xác định. (Xem mục C để tạo một Password vững chắc). Click Save. 6- Ghi vào giấy Password mới. Đóng Windows này. 7- click Forwarding &POP/IMAP. Xem Forward a copy of incoming mail to, cần xem kỹ không có tên email lạ ở mục này. Nếu có ghi vào giấy tên email lạ này, xóa bỏ, rồi click vào Disable forwarding. Click Save. Đóng windows.	1- click Options. Click Mail Options. 2- click Account Information. 3- click Update your Information (In ra giấy để lưu). Email 1 và email 2 là email mà khi quên password, khi được yêu cầu, Yahoo sẽ gửi email với cách reset password đến địa chỉ email này. Tất cả những chi tiết này đều cần để yêu cầu Yahoo giúp đỡ. 4- click Update Password reset info. Email 1 và email 2 là email mà khi quên password, khi được yêu cầu, Yahoo sẽ gửi email với cách reset password đến địa chỉ email này. 5- click Change your Password. Đánh máy vào Password hiện dùng. Đánh máy Password mới, đánh máy Password mới một lần nữa để xác định. (Xem mục C để tạo một Password vững chắc). Click Save. 6- Ghi vào giấy Password mới. Đóng Windows này. 7- click POP & Forwarding. Click Setup or edit POP & Forwarding. Cần xem kỹ không có tên email lạ ở mục này. Nếu có ghi vào giấy tên email lạ này, xóa bỏ, rồi click vào Web & POP Access. Click Save. Đóng windows.	1- Click Options. Click More Options. 2- Click View and edit your personal information . Click Registered information . Nếu cần thì nên thay đổi cho đúng, xong nên in ra giấy để lưu. Click Save. 3- Kiểm soát phần Password reset information. Chỗ Password, click Change. Đánh máy vào Password hiện dùng. Đánh máy Password mới, đánh máy Password mới một lần nữa để xác định. (Xem mục C để tạo một Password vững chắc). Click Save. 4- Chỗ Alternate e-mail address cần xem lại đúng hay không. Nếu cần thay đổi thì click Change để thay đổi. Đây là nơi khi xin password Hotmail sẽ gửi email tới để cho biết password mới.

Cả 3 công ty email này, hotmail là công ty có độ an toàn yếu nhất.

III- Tạo một Password vững mạnh:

Một Password vững mạnh (strong) là một Password khó phá. Hiện nay cả Hotmail, Yahoo, Google đều cho phép chúng ta dùng password dài. Password là tiền đồn, nếu tin tặc phá được password, tất cả tin tức trong email đều có nguy cơ bị lấy trộm và email của chúng ta có nguy cơ phải bị huỷ bỏ. Do đó việc xây dựng tiền đồn vững mạnh là điều quan trọng số một.

Sau đây là một số nguyên tắc:

- 1- Password phải dài, ít nhất phải có 12 mẫu tự và số (characters and numbers) trở lên. Lý tưởng là 20 chữ - số tổng cộng. Càng dài tin tặc càng phải mất nhiều thời gian hơn để phá. Thời gian phá tăng theo cấp số nhân so với chiều dài của Password.
- 2- Password phải gồm cả mẫu tự và số. Chữ gồm cả mẫu tự đầu như a b c, mẫu tự giữa như m n o và những mẫu tự cuối như x y z. Số phải gồm những số đầu, giữa và cuối.
- 3- Mẫu tự phải gồm cả mẫu tự hoa (upper case) và mẫu tự thường (lower case)
- 4- Một thí dụ: Password của tôi là Paris29Rome58LeCaire. Để dễ nhớ, tôi ghi Password ngoài sổ tay, và ngoài giấy để trước máy vi tính. Mỗi tuần đổi một lần. Có tuần dùng Paris29LeCaireRome5 8, có tuần chỉ thay đổi số, có tuần thay đổi thành phố khác. Còn số là số tuổi của con trai tôi và của tôi, v.v... Mục đích là tạo một cái gì đó logic một chút để dễ nhớ.
- 5- Nguyên tắc trên sử dụng cho cả Password của Windows và Password của email.
- 6- Mỗi một hay hai tuần phải đổi Password một lần.

C- Backup lại tên email trong Contact list:

Tin tặc sử dụng email của quý vị, lấy tên tất cả những người quen của quý vị có tên trong Contact list để gửi ra những bản tin có lợi cho chúng và có hại cho quý vị. Một người bạn của tôi năm rồi đã bị tin tặc lấy hotmail của chị gửi đi bản tin cho tất cả bạn bè quen biết yêu cầu gửi tiền gấp vì chị đã bị mất hết giấy tờ đang đi du lịch ở Hy Lạp nay không có tiền trở về. Anh bạn abcdef của tôi tuần qua Hotmail của anh cũng bị tin tặc lấy Contact list và gửi đến những người quen các tin tức không cần thiết.

Do đó, ngay bây giờ, quý vị hãy:

- 1- click vào Contact của email mình, export contact list này qua dạng Outlook, save vào một chỗ nào đó bằng cái tên mình chọn.
- 2- open hồ sơ này. Microsoft Excel sẽ mở Contact list này. Kiểm soát lại chắc chắn. Xong trở về Contact list trong email, highlight toàn bộ tên. Delete hết tất cả các tên này.
- 3- Mỗi khi cần một tên nào đó, đành phải mở Excel lên rồi copy email ra paste vào email.

D- Một số biện pháp khác để hỗ trợ:

1- Password: Không cài *nhớ password*, chịu khó đánh máy mật mã vào máy mỗi khi cần mở email. Mật mã phải thay đổi một tháng hay nửa tháng một lần. Thí dụ thay đổi Mật mã Windows tuần 1 thì thay đổi mật mã Email tuần 2. Xen kẽ như vậy. Sử dụng password mạnh cho máy tính và cho emails. Cần thay đổi thường xuyên.

2- Mỗi ngày cần kiểm Settings của email:

- a- Đối với Yahoo: xem B Yahoo 7 để biết chắc là email của mình không bị chuyển đi nơi khác.
- b- Đối với Google: xem B Google 7 để biết chắc là email của mình không bị chuyển đi nơi khác.
- c- Đối với Hotmail: xem B Hotmail 4 để biết chắc là email của mình không bị chuyển đi nơi khác.

3- Mỗi người cần sử dụng 2 hay 3 emails khác nhau.

- a- Email sử dụng cho những dịch vụ tối quan trọng cần thay đổi mật mã liên tục mỗi tuần một lần.
- b- Email sử dụng cho những dịch vụ quan trọng: thay đổi mật mã thường nhưng không cần mỗi tuần một lần. Một tháng hay hai tuần một lần cũng tạm an toàn.
- c- Email sử dụng cho những dịch vụ công cộng: giao tiếp công chúng, vào các web site, vào blogs hay những nơi như facebook, skype, Paltalk, ... Emails sử dụng cho những dịch vụ này không cần độ an toàn quá cao.

Cần có sổ để bàn ghi những mật mã đang sử dụng. Cần ghi lại những chi tiết cần thiết để khi quên mật mã, mình có thể xin mật mã được.

4- Sử dụng Outlook:

Chúng ta cần làm quen hay học cách sử dụng Outlook. Cách an toàn nhất là sử dụng Outlook với những biện pháp sau đây:

- a- Chuyển tất cả các mails vào email tới Outlook. Outlook tự động xoá mail trong email.
- b- Hồ sơ Outlook cần nằm ngoài Hard Drive cầm tay. Khi không sử dụng chúng ta rút dây ra.
- c- Với Outlook, chúng ta có thể soạn mail sẵn khi không on-line. Khi nào on-line chúng ta gửi mails đi một lượt.
- d- Cài đặt sao cho Outlook lấy mails từ email của chúng ta vào máy. Mỗi ngày hay mỗi vài ngày, chúng ta cần chuyển tất cả những mail trong máy sang Hộp thư trong Hard Drive rời.

5- Sử dụng Hard disk cầm tay:

Máy và Email có thể bị tấn công bất cứ lúc nào. Cách an toàn nhất là luôn đặt trong tình trạng máy bị trục trặc bất ngờ và mất tất cả tin tức. Vậy chúng ta cần ngăn ngừa ra sao?

a- sử dụng Hard disk cầm tay. Hiện nay Hard disk cầm tay loại nhỏ bằng bàn tay, nổi máy vi tính bằng dây USB, giá rất rẻ, chỉ 80AUD một hard disk 320Gb nhẹ vài trăm grams. Chúng ta save tất cả tài liệu vào một hay hai ba hard disk loại này (Hard disk trong máy để trống, chỉ chứa những tài liệu phỏ bản, nếu bị đánh cắp hay bị mất cũng chẳng sao).

b- email và tất cả tài liệu quan trọng đều giữ trong hard disk này. Chúng ta set up Outlook để Outlook save mail vào Hard disk cầm tay và chuyển thói quen làm việc với Outlook hơn là làm việc với Yahoo, Google trực tiếp.

6- Email bị chặn giữa đường:

Email của chúng ta có thể bị tin tặc chặn giữa đường. Một số email của chúng ta không tới được tay người nhận. Để bảo đảm đường dây liên lạc được tốt chúng ta cần tập lại thói quen trả lời sau khi nhận email cá nhân. Chỉ cần trả lời ngắn gọn: "Noted", "Đã nhận", ... để người gửi biết rằng email đã tới tay người nhận. Có rất nhiều emails của tôi gửi đi, khi hỏi lại mới biết trong cùng một mail list một số người không nhận được email trong khi một số người khác lại nhận được. Do đó việc trả lời giúp người gửi yên tâm và cũng là cách xác nhận email đã tới tay để người gửi được an lòng.

E- KẾT LUẬN:

Võ quýt dày có móng tay nhọn. Không có biện pháp nào là an toàn vĩnh viễn. Tất cả các biện pháp trên đây chỉ làm khó tin tặc và hoàn toàn không có nghĩa là tin tặc không xâm nhập được email của chúng ta. Chúng sẽ xâm nhập được, nhưng không còn dễ dàng nữa. Khi mà tất cả chúng ta đều sử dụng password mạnh, thay đổi thường xuyên và với sự cảnh giác cao độ như đã trình bày ở trên, chắc chắn tin tặc sẽ chẳng thu được lợi ích gì đáng kể sau khi mất cả hai ba ngày để phá password của một email. Khi ấy chúng sẽ xoay sang biện pháp khác.

Điều quan trọng là dù bất cứ tình huống nào, khi biết được email của tin tặc, hãy gọi hay email cho Google hay Yahoo và các cơ quan chức năng khác báo cho họ biết địa chỉ email của tin tặc sử dụng để họ tìm ra ngay cái máy điện toán đã sử dụng email này. Đối với chúng ta, nhiều lắm chúng ta chỉ có thể biết tên IP nhưng không biết IP đó ở địa chỉ nào, các cơ quan chức năng sẽ làm được chuyện này giúp chúng ta. Và đó cũng là cách để giữ gìn sự an toàn cho xã hội tốt đẹp nơi chúng ta sinh sống, những nơi này phải hoàn toàn miễn nhiễm với những thói tính xấu xa, tội ác và thủ đoạn phá hoại của Cộng Sản.