BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CẨM NANG AN TOÀN THÔNG TIN

CHO CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC

An toàn thông tin có ý nghĩa hết sức quan trọng đối với người sử dụng công nghệ thông tin nói chung và cán bộ, công chức, viên chức nói riêng. Các nguy cơ mất an toàn thông tin không chỉ ảnh hưởng đến các cá nhân mà còn có tác động mạnh mẽ đến sự phát triển và ổn định của xã hội.

Do đó, các cán bộ, công chức, viên chức cần tự trang bị các kiến thức cơ bản nhằm tự bảo vệ mình trước các nguy cơ mất an toàn thôn tin vốn ngày càng phức tạp hiện nay.

Cẩm nang mong muốn cung cấp các thông tin và kĩ năng cơ bản nhất về một số nguy cơ mất an toàn thông tin phổ biến trong việc sử dụng thiết bị và dịch vụ công nghệ thông tin

Hà Nội 2015

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

CẨM NANG AN TOÀN THÔNG TIN

CHO CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC

Hà Nội 2015

MỤC LỤC

CÁC BƯỚC THIẾT LẬP MÁY TÍNH MỚI AN TOÀN

- **Các nguy cơ mất an toàn thông tin có thể lập tức ảnh hưởng đến chúng ta ngay sau khi sử dụng máy tính vừa mua hoặc vừa cài đặt lại.**
- **Do đó cần có một số lưu ý để thiết lập máy tính mới an toàn chống lại các nguy cơ bị tấn công như sau:**

Bước 1: Tạo các mật khẩu mạnh.

Ngay trong các bước đầu tiên của việc thiết lập cấu hình máy tính. Các tài khoản của người sử dụng cần được tạo ra với mật khẩu có độ phức tạp nhất định.

Các mật khẩu dễ nhớ như "123456", "abcdef" ... tuyệt đối không được sử dụng vì đây là các mật khẩu yếu rất dễ đoán. Một mật khẩu an toàn thường bao gồm các loại ký tự sau:

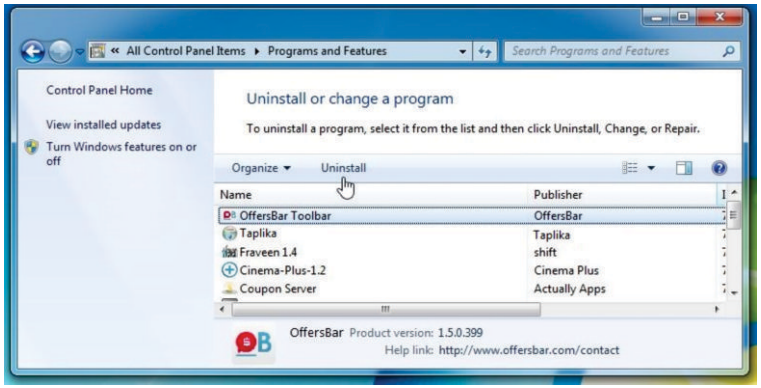
- ký tự hoa, ký tự thường
- ký tự chữ số
- ký tự đặc biệt ($#%"#%)

Mật khẩu mạnh sẽ giúp bảo vệ máy tính trong suốt quá trình sử dụng về sau

Bước 2: Tháo gỡ các chương trình không cần thiết.

Các máy tính mới thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm. Các phần mềm này có thể chứa sẵn các nguy cơ mất an toàn thông tin.

Do đó, người dùng cần tháo bỏ các chương trình không cần thiết trên máy tính của mình ngay trong quá trình thiết lập ban đầu .

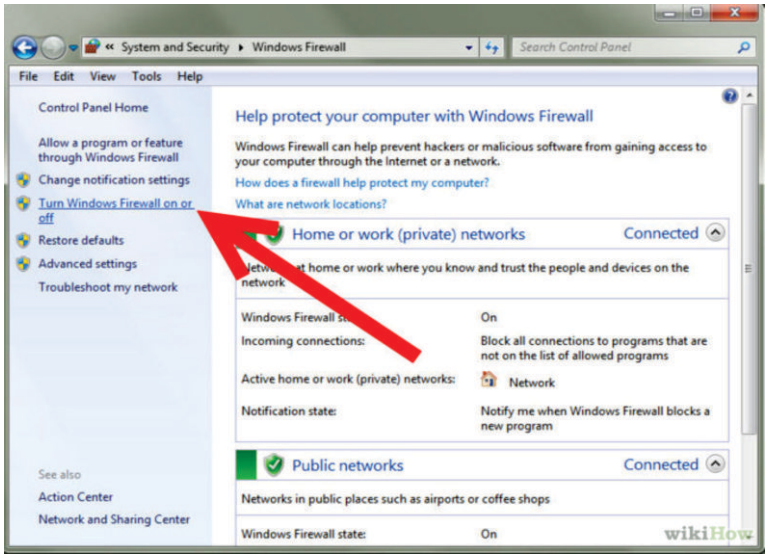


(Sử dụng chức năng Programs and Features để liệt kê các phần mềm đã được cài sẵn trong các máy mới)

Bước 3: Kích hoạt chức năng tường lửa bảo vệ cá nhân trên máy tính.

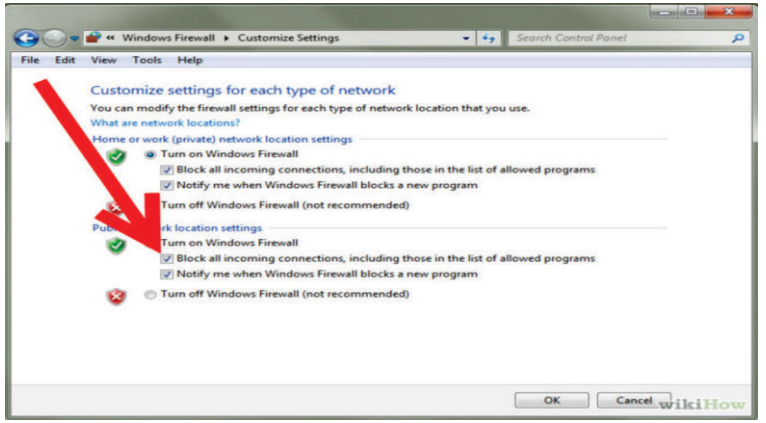
Các hệ điều hành hiện nay hầu hết đều tích hợp các tường lửa nhằm bảo vệ người sử dụng khỏi các tấn công cơ bản. Hãy kích hoạt phần mềm tường lửa trước khi kết nối đến bất kỳ mạng máy tính nào (Internet/Wifi/LAN...).

Trên hệ điều hành Windows, có thể kích hoạt tường lửa bằng cách truy cập chức năng Firewall trong Control Panel:



(Bảng điều khiển của chức năng Control Panel)

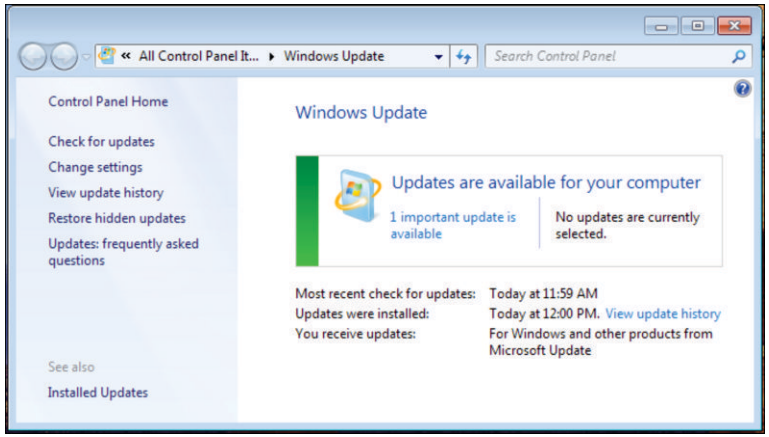
Tiếp tục lựa chọn "Turn Windows Firewall on or off" để thực hiện việc kích hoạt.



Tiếp tục chọn các lựa chọn "Turn on.." và tuỳ chọn bên dưới để kích hoạt.

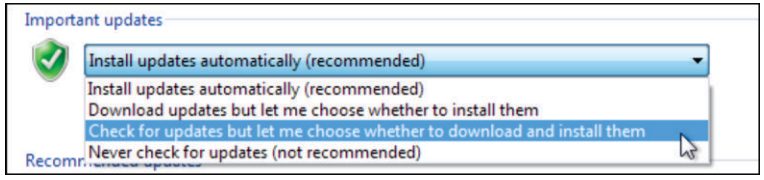
Bước 4: Nâng cấp các phần mềm và hệ điều hành Windows.

Hệ điều hành của máy tính lúc vừa cài đặt có thể là phiên bản cũ chưa được vá các lỗi bảo mật. Do đó, người sử dụng cần thiết lập chế độ tự động nâng cấp và thực hiện nâng cấp cho hệ điều hành và các phần mềm khác.

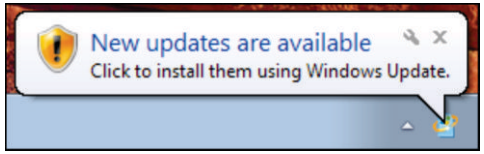


Trong phần Windows update của Control Panel, sử dụng tuỳ chọn "change settings" để thiếp lập việc tự động cập nhật.

Trong các tuỳ chọn về nâng cấp, người sử dụng có thể tuỳ chọn theo nhu cầu của mình. Tuy nhiên, có thể tuỳ chọn việc tự quyết định thực hiện nâng cấp theo yêu cầu của người sử dụng để đảm bảo không bị gián đoạn công việc do quá trình nâng cấp.



Sau đó, máy tính sẽ thông báo đến người sử dụng khi có bản cập nhật mới. Người sử dụng sẽ click vào thông báo để thực hiện việc cập nhật.



Bước 5: Cài đặt phần mềm diệt virus

Phần mềm diệt virus là lớp lá chắn quan trọng bảo vệ người sử dụng khỏi các mã độc và virus. Do đó, cần có chương trình diệt virus để bảo vệ người dùng ngay trong các hoạt động đầu tiên của người sử dụng trên máy tính.

Trên thị trường có nhiều hãng cung cấp giải pháp diệt virus, người sử dụng có thể lựa chọn chọn giải pháp miễn phí hoặc các giải pháp thương mại.

(Một số hãng phần mềm diệt virus nước ngoài)

Ngoài ra, người dùng có thể cân nhắc sử dụng các phần mềm diệt virus của Việt Nam sản xuất như BKAV hay CMC. Các phần mềm này đều có các phiên bản miễn phí với chức năng hạn chế cho người sử dụng.

(Phần mềm diệt virus BKAV)

(Phần mềm diệt virus CMC)

AN TOÀN THÔNG TIN KHI SỬ DỤNG MẠNG KHÔNG DÂY

Trong những năm gần đây, mạng không dây ngày càng trở nên phổ biến, giá thành thấp và dễ sử dụng. Người dùng có thể lắp đặt để truy cập mạng không dây tại nhà hoặc sử dụng máy tính xách tay, thiết bị di động thông minh để truy cập tại những nơi công cộng như quán café, sân bay, khách sạn...

Việc sử dụng mạng không dây sẽ rất tiện lợi và đơn giản nhưng nó cũng tiềm ẩn rất nhiều nguy cơ mất an toàn thông tin.

Nếu mạng không dây không được bảo vệ đúng mức thì bất cứ một máy tính nào có hỗ trợ truy cập không dây nằm trong vùng phủ sóng của thiết bị phát sóng đều có thể kết nối để truy cập Internet. Ở ngoài trời, phạm vi này có thể đạt tới hơn 300m. Vì vậy, bất cứ ai ở xung quanh cũng có thể dễ dàng truy cập vào thiết bị phát sóng này.

CÁC NGUY CƠ CÓ THỂ XẢY RA:

1. Bị xâm phạm dịch vụ: dung lượng, số lượng kết nối ... có thể vượt quá giới hạn mà nhà cung cấp dịch vụ cho phép, tốc độ có thể rất chậm do bị chiếm dụng băng thông.
2. Bị lợi dụng: một số người có thể lợi dụng hệ thống để thực thi những hành động bất hợp pháp.

❸ Bị theo dõi: các hoạt động trên internet có thể bị theo dõi, những thông tin nhạy cảm (mật khẩu, số thẻ tín dụng có thể bị đánh cắp).

❹ Bị tấn công: các tệp tin trên máy tính có thể bị truy cập trái phép, máy tính có thể bị cài đặt spyware và các chương trình độc hại khác.

Những việc cần làm khi truy cập Internet bằng mạng không dây công cộng

1. *Sử dụng mạng riêng ảo*

Yếu tố đầu tiên phải kể đến trong mặt tốt của mạng không dây là sự tiện lợi, dễ dàng sử dụng mà không cần phải thiết lập hay cấu hình gì quá phức tạp. Tuy nhiên, yếu tố an ninh trong mạng không dây thường vẫn bị cho qua.

Khi đã kết nối laptop hay điện thoại của mình vào một mạng mạng không dây nào đó, thì tất cả những thiết bị trong cùng mạng này có thể nhìn thấy nhau. Đây là điều hoàn toàn có lợi cho những kẻ xấu đang kết nối vào cùng mạng không dây, chúng có thể đánh cắp thông tin tài khoản hay xem trộm dữ liệu cá nhân của người dùng trong mạng.

Do vậy, ưu tiên số một khi sử dụng mạng không dây là nên cài đặt mạng riêng ảo (VPN - Virtual Private Network) cho truy cập của mình.

Khi sử dụng VPN để truy cập Internet, nó sẽ tự động thiết lập một kết nối mạng dựa trên chính nền tảng mạng mạng không dây nhưng đã được mã hóa các gói tin truyền đi và nhận về, đồng thời chuyển hướng truy cập giúp người dùng ẩn danh dễ dàng trên Internet. Tuy nhiên, chính vì yếu tố bảo mật cao này mà VPN sẽ làm suy giảm một phần tốc độ mạng.

2. *Sử dụng xác thực 2 bước*

Để tiện cho người dùng truy cập vào mạng không dây, những người quản trị mạng ít khi thiết lập bảo mật nghiêm ngặt cho mạng không dây. Đa phần chỉ chọn cách đặt mật khẩu đơn giản là những chuỗi số dễ nhớ, hay một cụm từ. Tức là, người dùng nào cũng có thể ghi nhớ và thuận tiện truy cập lại cho lần sử dụng tiếp theo.

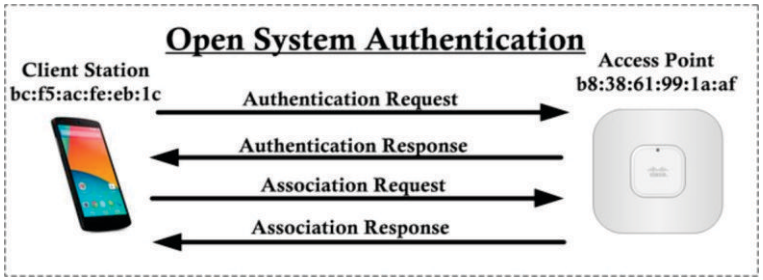
Thông thường, khi đã truy cập vào mạng Internet, đa số người dùng đều đăng nhập vào các tài khoản chứa nhiều thông tin cá nhân,ví dụ như email. Do đó, nếu đã không chọn sử dụng kết nối VPN, và nếu tài khoản email thiết lập lỏng lẻo, thì điều này chẳng khác nào mời gọi những kẻ xấu tìm đến!

Do đó, luôn sử dụng cơ chế xác thực 2 bước cho những tài khoản của mình. Thậm chí, để an toàn hơn, nên chọn cách xác thực bằng số điện thoại cá nhân, thay vì những câu hỏi bí mật đơn giản.

Ví dụ, nếu chọn kích hoạt xác thực 2 bước cho tài khoản Gmail, thì sau khi nhập đúng mật khẩu bạn vẫn phải chờ Gmail gửi thêm một tin nhắn SMS đến điện thoại của người dùng. Tin nhắn đó sẽ cung cấp số mật mã từ phía Google để nhập vào rồi mới đi vào được hộp thư.

3. *Cẩn thận với tính năng tự động kết nối mạng không dây*.

Một trong những mặt tốt và cũng là nguy cơ tiềm ẩn biến người sử dụng trở thành miếng mồi ngon cho kẻ xấu chính là cơ chế ghi nhớ kết nối mạng không dây của điện thoại, máy tính. Mặc định, khi dùng thiết bị kết nối vào một mạng không dây nào trước đó, thì điện thoại hay laptop sẽ tự động kết nối cho những lần sau. Thật vậy, sau này, mỗi khi thiết bị đó ở trong phạm vi của mạng không dây đó thì nó sẽ dò và kết nối vào một cách tự động. Lợi dụng cơ chế này, kẻ xấu có thể đoán biết thói quen này của người dùng để lấy cắp dữ liệu mà người dùng không ngờ đến.



Bên cạnh đó, cũng có những mạng không dây không đặt mật khẩu truy cập, chỉ cần chọn mạng không dây là kết nối vào. Khi đó, việc tấn công sẽ trở nên đơn giản và dễ dàng hơn rất nhiều.

4. *Xác minh mạng không dây*

Hãy luôn là người dùng thông minh bằng cách kiểm chứng tên kết nối trước khi truy cập. Kẻ xấu có thể đặt tên cho mạng không dây giả của họ gần giống, hay giống hoàn toàn như tên mạng mà bạn thường sử dụng. Nếu không cẩn thận, người dùng sẽ hướng luồng truy cập của mình tới

nhầm hướng; khi đó, những gì người dùng gửi đi cũng như nhận lại sẽ bị ghi nhận lại.

Cách tốt nhất là hãy luôn kích hoạt mạng riêng ảo trong mọi tình huống và tỉnh táo hơn nếu nhận thấy có dấu hiệu bất thường từ khâu kết nối. Nên liên lạc với quản trị của mạng không dây đó để xác thực cho chắc chắn hơn nữa.

5. *Hạn chế việc đăng nhập*

Đây có lẽ là yêu cầu khó thực hiện nhất, khi mà thời đại bùng nổ thông tin. Để an toàn, hãy tập thói quen hạn chế truy cập vào các tài khoản cá nhân khi đang dùng mạng không dây. Tức là, chỉ sử dụng mạng không dây để đọc báo, lướt web.

Nếu bắt buộc phải truy cập vào mail hay tài khoản mạng xã hội, hoặc giao dịch mua bán bất kỳ, hãy kích hoạt mạng VPN lên trước, đồng thời chỉ sử dụng các dịch vụ hỗ trợ giao thức HTTPS mà thôi. Với giao thức này, mọi thông tin của sẽ được an toàn hơn nhờ cơ chế mã hóa mà HTTPS hỗ trợ.

KỸ NĂNG PHÒNG CHỐNG MÃ ĐỘC

Mã độc là các phần mềm được thiết kế nhằm thực hiện các hoạt động gây hại cho người sử dụng công nghệ thông tin. Mã độc có thể tồn tại trên máy tính, điện thoại thông minh hay các thiết bị công nghệ thông tin khác.

Mã độc khi lây lan vào máy tính có thể thực hiện các hành vi như:

Lấy cắp dữ liệu:

Các dữ liệu quan trọng của người sử dụng như tệp tin văn bản mật, tệp tin nhật ký, hình ảnh riêng tư,... có thể bị mã độc lấy đi và bí mật gửi ra ngoài máy tính. Điều này đặc biệt quan trọng đối với các tổ chức, cơ quan nhà nước khi các tài liệu được xử lý bằng máy tính thường chứa dữ liệu nhạy cảm.

Theo dõi hoạt động:

Sau khi lây nhiễm vào máy tính, mã độc sẽ theo dõi hoạt động của người sử dụng trên máy tính này. Các hoạt động của người sử dụng như soạn văn bản, soạn thư điện tử, sử dụng mạng xã hội đều có thể bị theo dõi bởi mã độc. Một số mã độc còn có thể nghe lén âm thanh xung quanh thiết bị đã bị lây nhiễm.

Bị lợi dụng thực hiện tấn công đối tượng khác:

Sau khi đã lây nhiễm và chiếm quyền điều khiển thiết bị, mã độc có thể lợi dụng thiết bị này để tấn công vào đối tượng thứ 3. Việc này giúp mã độc che dấu nguồn gốc thông tin cũng như gây khó khăn cho quá trình điều tra. Một số cuộc tấn công liên quốc gia gây ra bởi mã độc có thể làm ảnh hưởng đến quan hệ ngoại giao cũng như uy tín của các quốc gia.

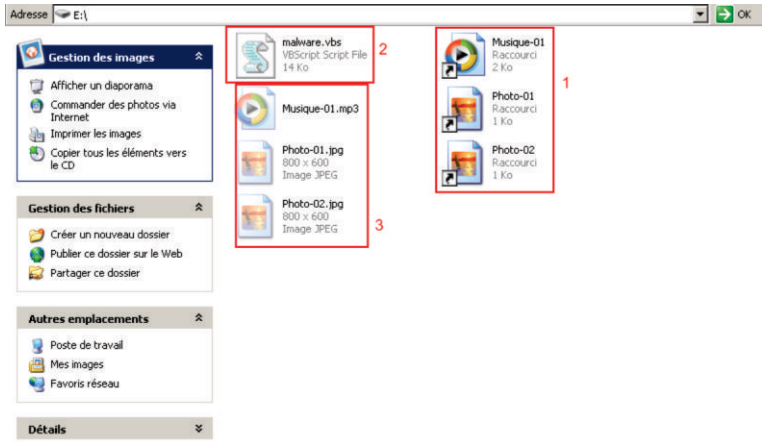
Phá hoại dữ liệu:

Các loại mã độc như mã độc tống tiền(ransomware) thường thực hiện mã hoá tất cả dữ liệu của người sử dụng và đòi hỏi phải chi trả chi phí để lấy lại dữ liệu. Trên thế giới và tại Việt Nam đã ghi nhận nhiều trường hợp phải chi trả số chi phí lớn để lấy lại các dữ liệu quan trọng phục vụ công việc và đời sống hàng ngày.

(Ví dụ về màn hình của máy tính đã bị nhiễm mã độc tống tiền)

(Ví dụ về màn hình của máy tính xuất hiện nhiều cửa sổ vì nhiễm mã độc)

(Máy tính nhiễm mã độc thường hay bị treo và lỗi)



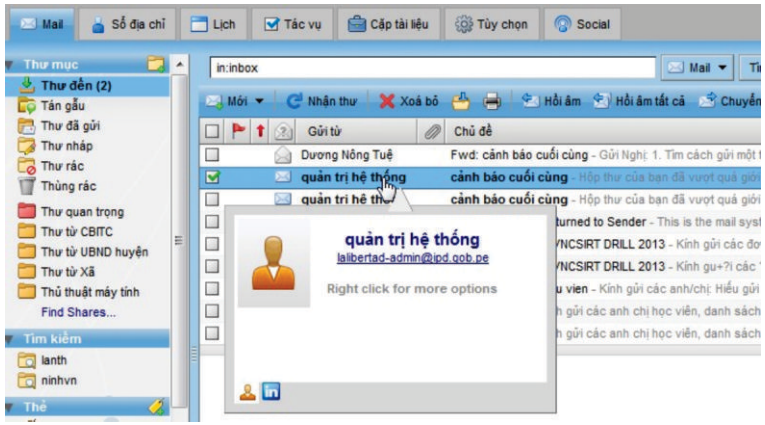
(Mã độc thường tạo ra các tệp tin lạ bất thường trên máy tính)

CÁC CÁCH PHÒNG CHỐNG MÃ ĐỘC

Chúng ta có thể phòng chống mã độc bằng một số biện pháp đơn giản như:

Sử dụng thư điện tử thận trọng

Mã độc có thể lây nhiễm vào máy tính người sử dụng thông qua các tệp tin đính kèm thư điện tử. Các tệp tin này thường được đính kèm các thư điện tử của người lạ gửi đến nạn nhân hoặc thư điện tử giả mạo một cơ quan tổ chức.



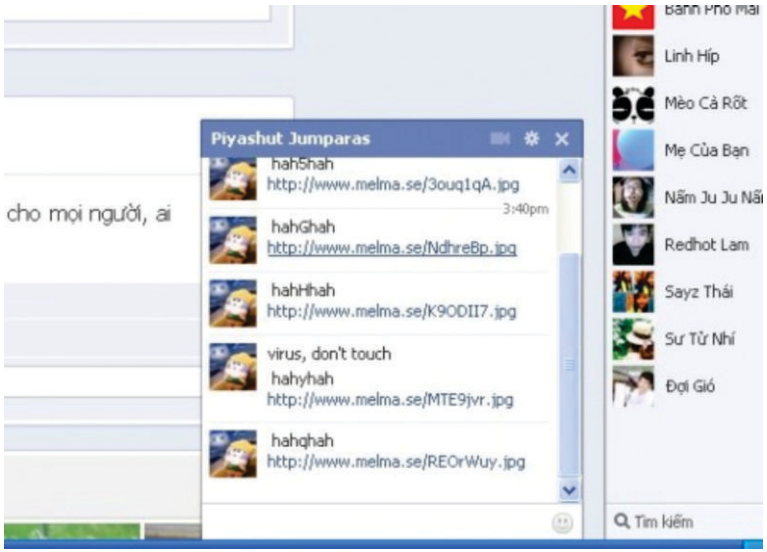
(Ví dụ một thư điện tử giả mạo đính kèm mã độc)

Do đó, người sử dụng **không nên mở** các tệp tin đính kèm thư điện tử nhận được từ một người lạ hoặc một người có địa chỉ thư điện tử giống với những người mà mình quen biết.

Ngoài ra, chúng ta có thể sử dụng chương trình diệt virus để dò quét tệp tin đính kèm trước khi đọc nội dung.

Cẩn thận khi truy cập các trang web trên mạng Internet

Chỉ cần truy cập vào một trang web độc hại là người dùng đã có thể bị lây nhiễm mã độc vào máy tính của mình. Các trang web này thường dụ dỗ người sử dụng truy cập thông qua các liên kết gửi qua mạng xã hội, thư điện tử hay tin nhắn. Vì vậy, người sử dụng cần thật cẩn trọng khi truy cập vào các trang web lạ được gửi đến từ người khác trong quá trình sử dụng các dịch vụ trên mạng Internet.



(Ví dụ về các liên kết độc hại gửi qua Facebook)

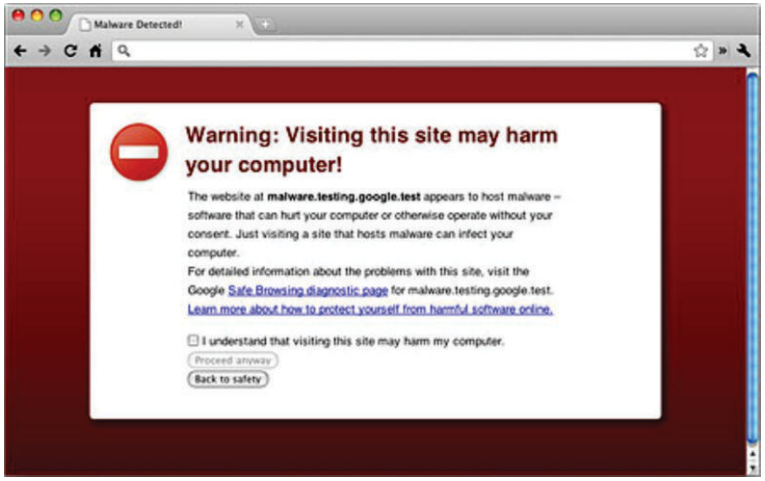
Thông Báo Sự Kiện

***HỆ THỐNG FACEBOOK MESSENGER Thông Báo:
Xin Chúc Mừng Tài Khoản Messenger Của Bạn Đã May Mắn
Trúng Được Giải Nhất Từ Trình Tri Ân Khách Hàng Tháng 3
Quý I Năm 2015. Tri Ân Khách Hàng Sử Dụng Mạng Xã Hội FaceBook.
Giải Thưởng Mà Bạn Nhận Được Trong Lượt Quay Số Ngẫu Nhiên Từ Hệ Thống Là:
1 Chiếc Xe Máy SH 125i & Phiếu Quà Tặng Trị Giá 100.000.000 VNĐ Tiền Mặt.

Quý Khách Vui Lòng Truy Cập Ngay Website: >>>>

(Ví dụ về tin nhắn lừa đảo giả mạo nhằm lừa người sử dụng truy cập vào trang web độc hại)

Hầu hết các trình duyệt Internet sẽ cảnh báo các trang web độc hại. Tuy nhiên, người sử dụng vẫn phải cảnh giác cho dù trình duyệt Internet không cảnh báo.

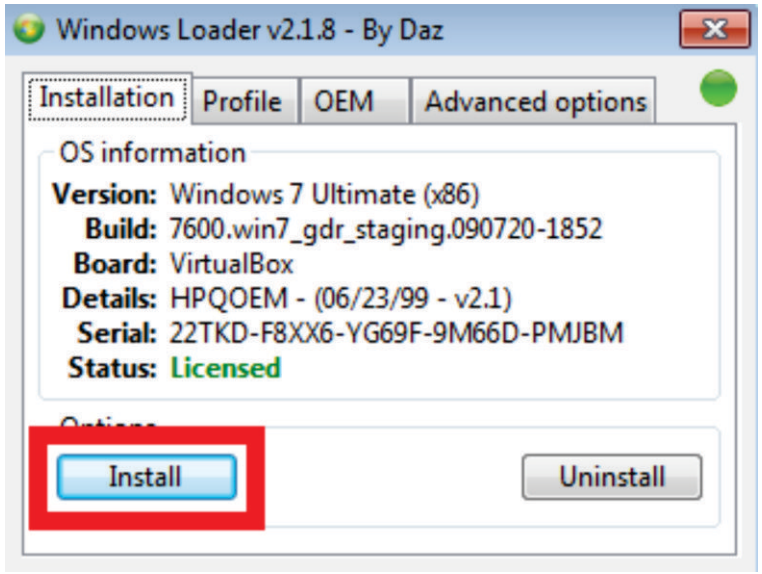


(Ví dụ về trình duyệt Internet cảnh báo khi truy cập trang web độc hại)

Không sử dụng phần mềm bẻ khoá, không bản quyền

Các phần mềm độc hại có thể tồn tại trong các phần mềm bẻ khoá, phần mềm miễn phí hay có trả phí nhưng không được tải từ chính trang web của nhà phát triển. Các phần mềm này thường được đính kèm virus, mã độc và sẽ được kích hoạt khi người dùng chạy các phần mềm này. Vì vậy, không nên tải, sử dụng hay cài đặt các phần mềm bẻ khoá hoặc các phần mềm được chia sẻ trên các diễn đàn, mạng xã hội mà người dùng không rõ nguồn gốc.

Cách tốt nhất để phòng chống mã độc là tải phần mềm tại ngay chính trang web của nhà sản xuất để tránh trường hợp tải phải phiên bản "giả mạo" kèm sẵn mã độc.



(Ví dụ về phần mềm bẻ khoá Windows có thể chứa mã độc)

(Các phần mềm keygen thường được đính kèm mã độc)

Sử dụng phần mềm diệt virus

Mỗi máy tính hay điện thoại cần được cài đặt các chương trình diệt mã độc. Các chương trình này sẽ tự động dò quét các tệp tin hay thư điện tử và cảnh báo người sử dụng khi phát hiện mã độc.

Trên thị trường hiện nay, có nhiều chương trình diệt virus miễn phí và có trả phí. Các chương trình miễn phí có ít chức năng hơn nhưng cũng có thể giúp người dùng cơ bản chống lại các mã độc thông dụng.

Một số chương trình diệt virus do Việt Nam sản xuất có khả năng bảo vệ tốt đối với người sử dụng Việt Nam.

(Cần cẩn trọng với việc sử dụng USB để sao lưu dữ liệu giữa các máy tính)

(Một số mã độc giả mạo chính phần mềm diệt virus. Do đó, người dùng cần tải các chương trình diệt virus tại chính trang web của nhà sản xuất)

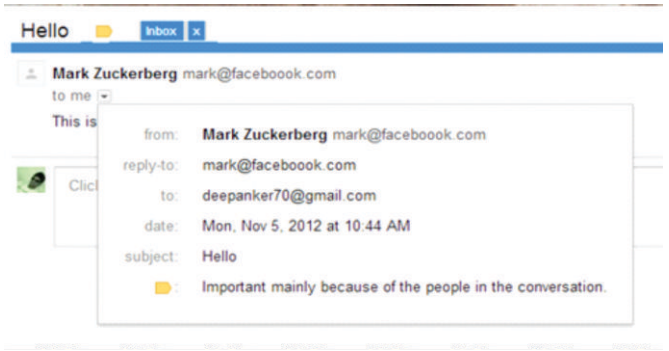
(Các phần mềm keygen thường được đính kèm mã độc)

HƯỚNG DẪN NHẬN BIẾT, PHÒNG CHỐNG THƯ RÁC, THƯ GIẢ MẠO, TIN NHẮN RÁC

Ghi nhớ thứ 1:
"Không nên tin tưởng tên hiển thị trong mail"

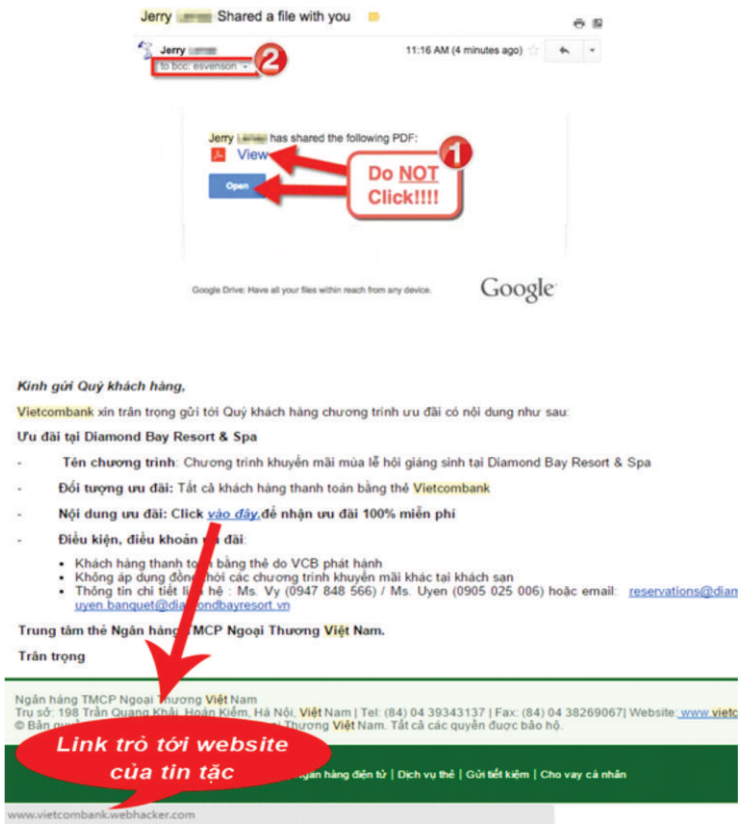
Một chiến thuật lừa đảo yêu thích của các tin tặc là giả mạo tên hiển thị của một email để đánh lừa người nhận được.

Các tên hiển thị hay được giả mạo như tên của các Công ty, tổ chức, hãng lớn; Người quen của bạn; Người nổi tiếng ...



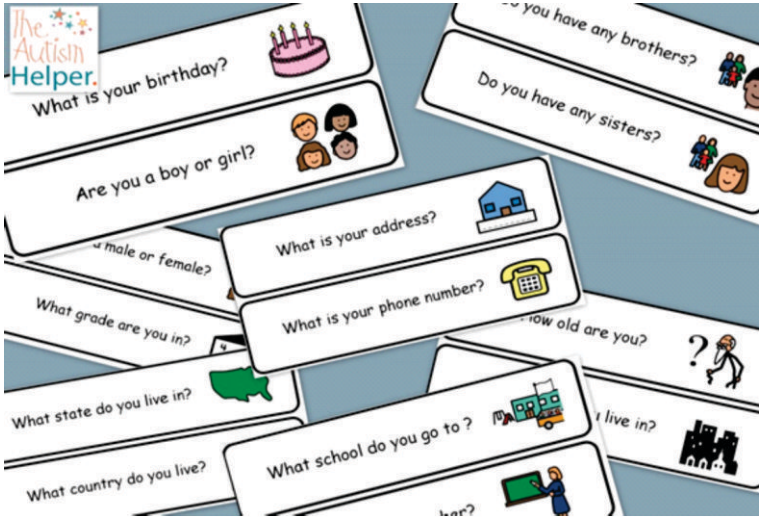
Ghi nhớ thứ 2:
"Cân nhắc kỹ lưỡng khi bấm vào liên kết (link) trong email"

Cẩn trọng khi bấm vào bất cứ liên kết (link) được gửi trong nội dung email. Liên kết (link) đó có thể dẫn bạn tới một website lừa đảo giả mạo, quảng cáo hay một website độc hại mà tin tặc dựng lên để tấn công.



Ghi nhớ thứ 3:
"Bỏ qua các email yêu cầu cung cấp thông tin cá nhân của bạn"

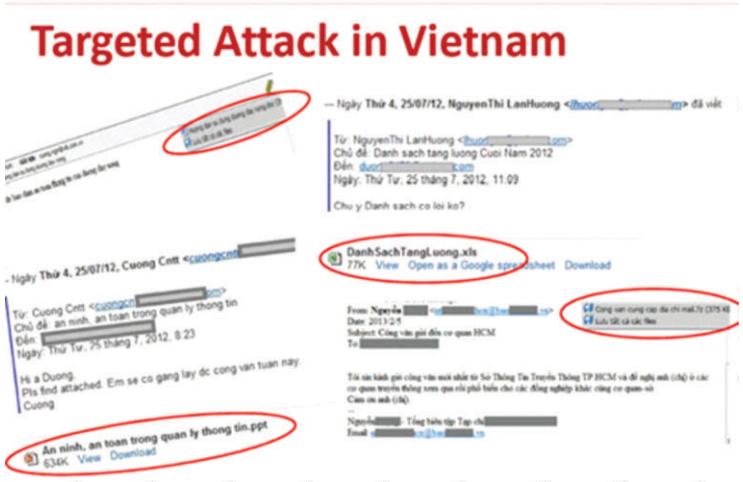
Một tổ chức, công ty, ngân hàng,...sẽ không bao giờ yêu cầu người sử dụng cung cấp thông tin cá nhân. Do vậy bạn hoàn toàn có thể bỏ qua chúng khi nhận được các email với nội dung đó.



Và thậm chí hạn chế tối đa, cân nhắc cẩn thận khi cung cấp thông tin cá nhân cho bất kỳ tổ chức nào.

Ghi nhớ thứ 4:
"Cẩn trọng với các email có tiêu đề Hấp dẫn - Nhạy cảm - Khẩn cấp"

Đánh vào tâm lý của người dùng, các tin tặc thường xuyên sử dụng các tiêu đề có tính Hấp dẫn – Nhạy cảm - Khẩn cấp trong email để lừa người dùng. Chúng ta bị tiêu đề đó làm chủ quan, mất cảnh giác, hay thậm chí là hoảng hốt và cảm thấy cần phải xử lý gấp. Ví dụ như: "Cập nhật bảng lương công ty Quý 2/2016" ; "Cảnh báo: Tài khoản của bạn bị đình chỉ" ...

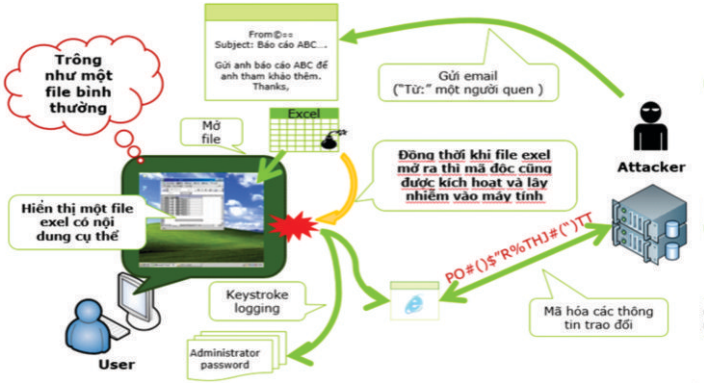


Ghi nhớ thứ 5:
"Cẩn thận, cân nhắc khi tải về các File đính kèm trong email

Tấn công bằng việc sử dụng cài mã độc, virus trong các file đính kèm trong email là phương thức tấn công phổ biến và nguy hiểm nhất hiện nay.

Không nên tải và mở chạy file ngay khi nhận được các email có file đính kèm.

Chú ý tới định dạng file và tạo thói quen quét virus với các file đính kèm trước khi mở chúng.



Ghi nhớ thứ 6:
"Nhận diện các email spam – email quảng cáo"

Bạn cần cảnh giác khi nhận các email spam, email quảng cáo từ Internet. Trong các email này thường đi kèm với nhiều rủi ro mất an toàn thông tin mà chúng ta không mong muốn như: lừa đảo, mã độc, gây ảnh hưởng tới công việc khi nhận quá nhiều...

Ghi nhớ thứ 7:
"Cẩn trọng với các tin nhắn rác"

Cũng tương tự như email spam thì các tin nhắn rác (sms spam) cũng gây cho người dùng rất nhiều phiền toái. Bên cạnh đó ngày nay các tin nhắn rác thường xuyên được sử dụng như một phương thức để lừa đảo người dùng như:

Bạn trúng thưởng một xe SH ....

Nhắn tin, gọi tới 1800XXXX, 1900XXXX, 1900XXXXXX, 6XXX, 7XXX, 8XXX, 9XXX,...

Truy cập vào đường link, trang web

Ghi nhớ thứ 8:
"Cần làm gì khi thường xuyên bị tin nhắn rác?"

Khi nhận được tin nhắn rác. Vui lòng gửi lại chúng tới đầu số miễn phí 456 của Bộ Thông tin và Truyền thông để được xử lý.

Sử dụng các ứng dụng chuyên chặn các tin nhắn rác trên thiết bị di động.

HƯỚNG DẪN SỬ DỤNG MẠNG XÃ HỘI AN TOÀN

Mạng xã hội là một dạng xã hội ảo, mục đích kết nối các thành viên cùng môi trường, công việc, sở thích trên mạng với nhau. Cho phép người dùng chia sẻ và giao lưu thông tin một cách hiệu quả.

Mạng xã hội có những tính năng như chat, e-mail, phim ảnh, chia sẻ file, blog và xã luận. Những dịch vụ này có nhiều phương cách để các thành viên tìm kiếm bạn bè, đối tác: dựa theo nhóm (ví dụ như tên trường hoặc tên thành phố), dựa trên thông tin cá nhân (như địa chỉ e-mail hoặc tên tài khoản), hoặc dựa trên sở thích cá nhân (như thể thao, phim ảnh, sách báo, hoặc ca nhạc), lĩnh vực quan tâm: kinh doanh, mua bán...

Hiện nay thế giới có hàng trăm mạng xã hội khác nhau, như MySpace và Facebook nổi tiếng nhất trong thị trường Bắc Mỹ và Tây Âu; Orkut và Hi5 tại Nam Mỹ; Friendster tại Châu Á và các đảo quốc Thái Bình Dương.

Tại Việt Nam xuất hiện rất nhiều các mạng xã hội như: Zing Me, YuMe, Tamtay...

Mạng xã hội có an toàn không?

Như xã hội thực tế, không một mạng xã hội trên Internet, thế giới ảo hay trò chơi trực tuyến nào đảm bảo được 100% an toàn cho người sử dụng.

Trong khi mạng xã hội được xem là phương tiện giao tiếp tốt với mọi người thì nó cũng trở thành mục đích cho tội phạm mạng. Các hãng bảo mật lớn đã quan sát được làn sóng đe dọa trực tuyến ngày càng tăng lợi dụng mạng xã hội để đánh cắp thông tin sử dụng cho mục đích kiếm tiền. Những đe dọa này ngày càng phức tạp hơn, khó phát hiện hơn và thường nhắm vào lối sống "kết bạn trực tuyến" của mọi người.

Các rủi ro khi sử dụng mạng xã hội

Mạng xã hội hoạt động trên nguyên tắc kết nối và chia sẻ thông tin. Do đó, các mạng xã hội sẽ bắt buộc người sử dụng phải cung cấp một số nhất định các thông tin cá nhân. Càng nhiều thông tin mà người sử dụng cung cấp lên mạng xã hội, càng làm tăng nguy cơ bị kẻ xấu lợi dụng:

- Làm ảnh hưởng tới hình ảnh, uy tín của bản thân.
- Sử dụng các thông tin đưa lên mạng xã hội như: vị trí địa lý, sở thích cá nhân, danh sách bạn bè, kẻ xấu có thể khai thác thêm các thông tin cá nhân khác hoặc các dữ liệu tài chính, ngân hàng của người dùng.
- Luôn luôn phải đối mặt với nguy cơ bị tấn công , bị cài phần mềm gián điệp làm lộ các thông tin mật của cá nhân hoặc cơ quan, tổ chức.
- Mạng xã hội có thể gây nghiện và có nguy cơ giành quá nhiều thời gian vào mạng xã hội, làm ảnh hưởng đến công việc và gia đình.

Làm sao để bảo vệ bản thân trên mạng xã hội?

- Luôn ghi nhớ, Internet là một mạng công cộng. Chỉ đưa những thông tin lên mạng khi mình thấy thoải mái cho mọi người có thể đọc, xem được những thông tin này. Khi công khai thông tin cá nhân của mình trên mạng xã hội, người sử dụng cần xác định những thành viên khác trên mạng xã hội và Internet đều có thể lấy được những thông tin này, kể cả trường hợp những thông tin này đã được xoá, chỉnh sửa thì các bản lưu có thể tồn tại ở máy tính của người sử dụng khác. Do vậy, người sử dụng cần giới hạn lượng thông tin cá nhân mà mình cung cấp lên mạng xã hội, cố gắng hạn chế công khai các thông tin có tính liên kết, xấu chuỗi với nhau.
- Bảo mật thông tin cá nhân trên mạng: không tiết lộ số điện thoại, địa chỉ thực tế, lịch công tác, thông tin liên quan tới công việc của mình tại cơ quan... Đặt chế độ cá nhân hoặc chỉ bạn bè thân thiết và tin cậy mới có thể xem để tránh trường hợp kẻ xấu có thể lợi dụng.

những thông tin đó uy hiếp, đe dọa. Sử dụng mật khẩu khó dò tìm, khó đoán và luôn giữ bí mật mật khẩu, tuyệt đối không chia sẻ cho ai khác.
- Xin phép bạn bè mình trước khi đăng tải những bức ảnh và các câu chuyện của họ. Tôn trọng người khác trong cộng đồng mạng.
- Suy nghĩ kĩ về những gì nói và đăng trên mạng
- Thể hiện sự tôn trọng người khác trong giao tiếp, ứng xử trên mạng. Tuyệt đối không nói xấu, bôi nhọ, kéo bè cánh nhằm hạ thấp danh dự của người khác, đề phòng những trường hợp trả thù ra ngoài cuộc sống thật.
- Đưa ảnh phù hợp lên mạng. Không đưa những hình ảnh hở hang, mang tính khiêu dâm hoặc mang tính chất bạo lực lên mạng. Kẻ xấu có thể sử dụng những bức hình đó cho những mục đích không tốt đẹp
- Sử dụng các trình duyệt web phổ biến và đã được cập nhật để truy cập mạng xã hội và Internet, thường xuyên theo dõi lịch sử truy cập để phát hiện các truy cập bất thường.
- Chỉ kết bạn với những người thân, quen biết ở ngoài đời. Xác minh với bạn bè, người thân qua điện thoại hoặc gặp mặt trước khi kết bạn trên mạng xã hội.
- Thường xuyên kiểm tra cơ chế bảo vệ thông tin cá nhân của mạng xã hội đối với tài khoản của mình. Kiểm tra các thông tin của tài khoản mà bạn bè, người lạ có thể thấy khi truy cập vào tài khoản của mình.
- Không nên đăng tải hoặc tag ảnh cá nhân hoặc người thân trong gia đình ở góc gần, chính diện.
- Không nên sử dụng cơ chế tự động đăng tải ảnh trên máy điện thoại di động, cho phép gắn vị trí địa lý vào các ảnh đã chụp.
- Không nên sử dụng ảnh chân dung, ảnh cá nhân làm hình đại diện trên mạng xã hội, thay vào đó, nên sử dụng ảnh hoạt hình hoặc các biểu tượng, ảnh minh hoạ khác.

Hướng dẫn thiết lập chế độ an toàn cho tài khoản Facebook

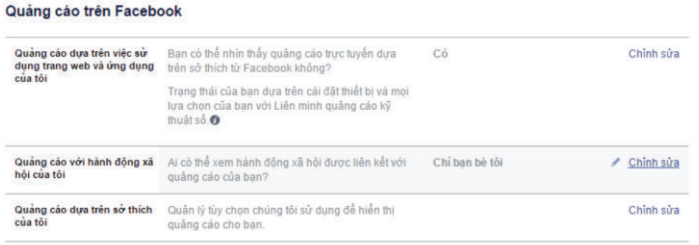
Các mục (1) Quyền riêng tư, (2) Dòng thời gian và gắn thẻ, (3) Bảo mật, (4) Quảng cáo đều chứa các tùy chỉnh liên quan tới thông tin cá nhân. Sử dụng các tùy chỉnh này để tăng cường an toàn cho tài khoản Facebook.

❶ Trong phần Quyền riêng tư, giới hạn người xem cho các bài viết trong tương lai tại phần "Ai có thể thấy các bài đăng sau này của bạn?". Kiểm tra các hoạt động của tài khoản Facebook tại mục "Sử dụng nhật ký hoạt động". Ẩn các bài viết cá nhân tại dòng thời gian hoặc thiết lập chế độ chỉ cho phép Bạn bè đọc.

❷ Click vào Dòng thời gian và gắn thẻ > "Xem với tư cách là" để thấy được những thông tin cá nhân của mình hiển thị với Bạn bè, người lạ trên Facebook như thế nào.

❸ Truy cập Bảo mật > "Địa điểm bạn đã đăng nhập" để xem xét các truy cập đối với tài khoản Facebook của mình. Khi xuất hiện các truy cập bất thường, click vào "kết thúc hoạt động" để ngăn chặn.

❹ Thiết lập "Quảng cáo với hoạt động xã hội của tôi" tại mục "Quảng cáo" về chế độ "chỉ bạn bè tôi".



THÔNG TIN LIÊN HỆ
CƠ QUAN QUẢN LÝ NHÀ NƯỚC VỀ AN TOÀN THÔNG TIN

TT	Họ tên	Chức vụ	Thông tin liên hệ
I	**Lãnh đạo Cục An toàn thông tin**		
1	Nguyễn Thanh Hải	Cục trưởng	043.9436999 thanhhai@mic.gov.vn
2	Nguyễn Huy Dũng	Phó Cục trưởng	043.9431555 nhdung@mic.gov.vn
3	Bùi Hoàng Phương	Phó Cục trưởng	043.9433779 bhphuong@mic.gov.vn
II	**Tổ đảm bảo an toàn thông tin, Cục An toàn thông tin**		
1	Trần Mạnh Thắng	Phó Giám đốc Trung tâm Tư vấn và Hỗ trợ nghiệp vụ ATTT	0963791366 tmthang@mic.gov.vn
2	Lê Bá Quốc Thịnh	Phó Trưởng phòng Thẩm định và Quản lý giám sát	091448884 9 lbqthinh@mic.gov.vn
3	Trần Đăng Khoa	Phụ trách phòng Kế hoạch - Tài chính	0904804803 tdkhoa@mic.gov.vn
4	Lê Văn Chương	Chuyên viên	098212378 9 chuonglv@mic.gov.vn

Chịu trách nhiệm nội dung
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CẨM NANG AN TOÀN THÔNG TIN

CHO CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC
(Lưu hành nội bộ)

In 500 cuốn, khổ 13x19cm tại Công ty cổ phần HD Hoàng Dương.
Số ĐKKHXB: 64B/GP-CXBIPH.
Cấp ngày 11-12-2015. In xong nộp lưu chiểu quý IV 2015.