HƯỚNG DẪN AN NINH MẠNG

Dịch vụ Ngân hàng trực tuyến (Internet Banking) là một dịch vụ tiện lợi và tiết kiệm thời gian. Quý khách có thể chuyển tiền, gửi tiền trực tuyến và thực hiện các giao dịch khác thông qua dịch vụ ngân hàng trực tuyến một cách thuận tiện và an toàn ngay tại nhà mình. Quý khách chỉ cần một chiếc máy tính có nối mạng internet để thực hiện tất cả các giao dịch này. Nhưng giống như tất cả các tiến triển về công nghệ khác, dịch vụ ngân hàng qua Internet cũng có một vài vấn đề Quý khách cần lưu ý như tội phạm nặc danh… Vì vậy, Quý khách cần biết những mối nguy hiểm thường gặp khi Quý khách sử dụng mạng trực tuyến cũng như các bước Quý khách cần thực hiện để bảo vệ chính Quý khách trước các mối đe dọa trên mạng như tội phạm tài chính và tội phạm nặc danh.

Những mối nguy hiểm trực tuyến thường gặp.

Vi-rút máy tính

Khi internet đang ngày càng trở nên phổ biến, tội phạm máy tính đã nhận thấy cơ hội để làm hại những người sử dụng thiếu cảnh giác nhằm lấy tiền của họ.

Bằng cách sử dụng các vi-rút máy tính và vi-rút Trojan, tội phạm máy tính tập trung và làm cho các máy tính không được bảo vệ bị nhiễm vi-rút để lấy quyền truy cập và mật khẩu khi Quý khách truy cập vào mạng internet. Các vi-rút này thường ghi lại các tiếng bàn phím, các nhắp chuột hoặc chụp nhanh màn hình của Quý khách mà không để Quý khách biết, khi Quý khách vào các trang web an ninh cần các thư ủy quyền của Quý khách và gửi các thông tin này tới các tội phạm máy tính đang chờ sẵn.

Vi-rút máy tính thường lan truyền qua các tài liệu đính kèm gửi qua e-mail (bao gồm cả các đường link dẫn đến kết nối vào các trang web) mà bề ngoài nhìn như là được gửi tới bởi một người quen của Quý khách hoặc một nguồn đáng tin cậy, và các dữ liệu được tải xuống từ internet.

Mẹo

Mỗi một máy tính dùng để truy cập vào dịch vụ Ngân hàng trực tuyến cần cài một ứng dụng an ninh mạng để bảo vệ Quý khách khỏi các vi-rút.

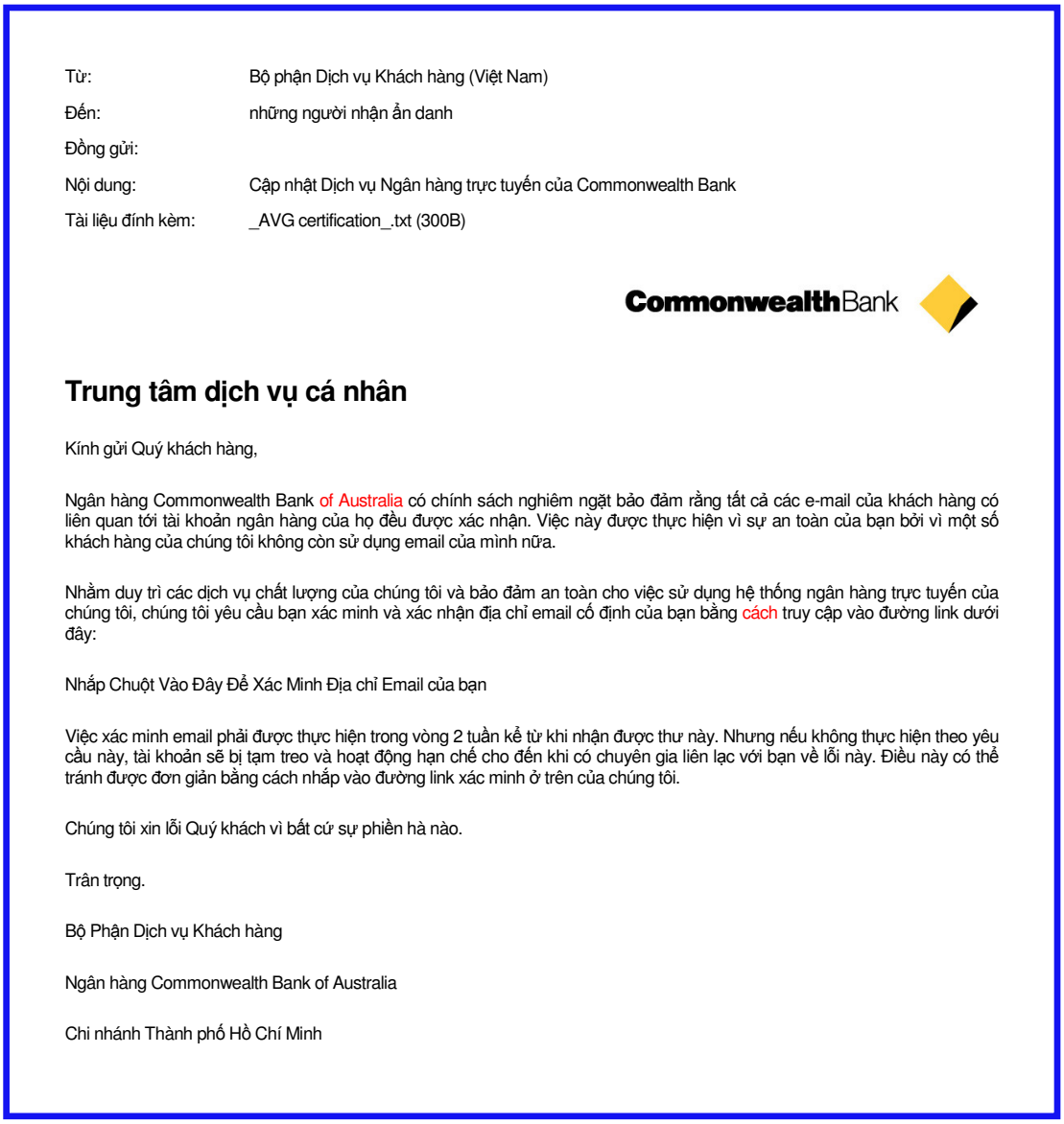
Các e-mail lừa đảo và gian lận

E-mail là một phương pháp tuyệt vời để liên lạc với bạn bè và gia đình. Thật không may, tội phạm cũng lợi dụng tính phổ biến của email để nhằm vào các khách hàng không cảnh giác bằng các thông điệp giả mạo để lấy các thông tin cá nhân hay tiền của họ.

Các email lừa đảo, thường được biết là phishing, có thể nhìn bề ngoài như là được gửi từ Ngân hàng Commonwealth Bank of Australia và yêu cầu Quý khách cập nhật hoặc xác nhận các thông tin như:

- Mã người sử dụng myAccess
- Mật khẩu thiết bị bảo mật myAccess
- Các câu hỏi nhận dạng cá nhân
- Các thông tin liên lạc
- Các số tài khoản

Ngân hàng Commonwealth Bank of Australia sẽ **không bao giờ** gửi Quý khách email yêu cầu Quý khách xác nhận, cập nhật hay cho biết thông tin ngân hàng bảo mật của Quý khách. Quý khách có thể xem một mẫu thư lừa đảo dưới đây:



Từ: Bộ phận Dịch vụ Khách hàng (Việt Nam)

Đến: những người nhận ẩn danh

Đồng gửi:

Nội dung: Cập nhật Dịch vụ Ngân hàng trực tuyến của Commonwealth Bank

Tài liệu đính kèm: _AVG certification_.txt (300B)

CommonwealthBank

Trung tâm dịch vụ cá nhân

Kính gửi Quý khách hàng,

Ngân hàng Commonwealth Bank of Australia có chính sách nghiêm ngặt bảo đảm rằng tất cả các e-mail của khách hàng có liên quan tới tài khoản ngân hàng của họ đều được xác nhận. Việc này được thực hiện vì sự an toàn của bạn bởi vì một số khách hàng của chúng tôi không còn sử dụng email của mình nữa.

Nhằm duy trì các dịch vụ chất lượng của chúng tôi và bảo đảm an toàn cho việc sử dụng hệ thống ngân hàng trực tuyến của chúng tôi, chúng tôi yêu cầu bạn xác minh và xác nhận địa chỉ email cố định của bạn bằng cách truy cập vào đường link dưới đây:

Nhấp Chuột Vào Đây Để Xác Minh Địa chỉ Email của bạn

Việc xác minh email phải được thực hiện trong vòng 2 tuần kể từ khi nhận được thư này. Nhưng nếu không thực hiện theo yêu cầu này, tài khoản sẽ bị tạm treo và hoạt động hạn chế cho đến khi có chuyên gia liên lạc với bạn về lỗi này. Điều này có thể tránh được đơn giản bằng cách nhấp vào đường link xác minh ở trên của chúng tôi.

Chúng tôi xin lỗi Quý khách vì bất cứ sự phiền hà nào.

Trân trọng.

Bộ Phận Dịch vụ Khách hàng

Ngân hàng Commonwealth Bank of Australia

Chi nhánh Thành phố Hồ Chí Minh

Hãy gửi các thư Quý khách nghi ngờ là thư lừa đảo theo dạng văn bản đính kèm đến chúng tôi tại địa chỉ email customerservice@commbank.com.vn và cho chúng tôi biết tình huống của Quý khách. Nếu Quý khách đã trả lời một thư lừa đảo, hãy nhanh chóng liên lạc Bộ phận Trợ giúp myAccess ngay lập tức theo số +84 8 3824 1525.

Các thư lừa đảo hứa hẹn cách kiếm số tiền lớn một cách nhanh chóng và dễ dàng. Có rất nhiều loại email lừa đảo khác nhau và luôn xuất hiện những thư lừa đảo kiểu mới, dưới đây là những mẫu thư lừa đảo thường được sử dụng:

'Nigerian 419' scams hứa hẹn các phần thưởng tài chính lớn nếu Quý khách giúp ai đó chuyển tiền ra khỏi nước họ bằng cách trả phí và cho họ biết các thông tin tài khoản ngân hàng của Quý khách.

Thư lừa đảo thanh toán trước yêu cầu Quý khách gửi tiền trước cho một sản phẩm hoặc "phần thưởng". Cuối cùng Quý khách sẽ nhận được cái gì đó không như Quý khách mong đợi hoặc không có gì cả.

Chuyển tiền cho một ai đó là cách cơ bản để tội phạm dùng tài khoản của Quý khách cho mục đích "rửa" tiền bẩn của chúng – giao dịch này là phi pháp và Quý khách có thể bị truy tố.

Mẹo

Các email lừa đảo nhìn bề ngoài quá thật đến không thể tin được – và bởi vì đấy chính là những thư lừa đảo!

Tội phạm nặc danh

Tội phạm nặc danh xảy ra khi các tội phạm dùng các thông tin cá nhân của Quý khách để trục lợi – bằng cách mạo nhận là Quý khách để nộp đơn xin vay, dùng hết các hóa đơn và không trả cho nhà cung cấp tín dụng.

Loại tội phạm này sử dụng các vi-rút, email lừa đảo và các địa chỉ mạng xã hội (trình bày dưới đây) để thu thập các thông tin cần thiết nhằm "lấy cắp" thông tin nhận dạng của Quý khách như tên, thông tin thẻ tín dụng, địa chỉ, ngày sinh, tài khoản ngân hàng, thông tin thẻ ghi nợ và giấy phép lái xe, và sau đó thực hiện hành vi lừa đảo bằng tên Quý khách.

Mạng xã hội

Các trang mạng xã hội như Facebook, MySpace và LinkedIn, là các cộng đồng mạng chia sẻ các mối quan tâm và các hoạt động với nhau và đưa ra rất nhiều cách để kết nối và liên lạc với những người khác. Thật không may những trang mạng này cũng cho các tội phạm một cách khác để lấy các thông tin phục vụ cho tội phạm nặc danh.

Để bảo vệ chính Quý khách khi sử dụng các trang mạng xã hội này, Quý khách cần:

- Đảm bảo các trang hồ sơ cá nhân của Quý khách chỉ có thể truy cập được bởi những người mà Quý khách tin cậy mà không phải cộng đồng chung bằng việc thay đổi cài đặt các chế độ an ninh.

- Không bao giờ đăng các thông tin cá nhân và các thông tin nhạy cảm như ngày sinh, số giấy phép lái xe, số hồ sơ thuế hay thông tin tài khoản ngân hàng.
- Không được đăng các thông tin liên lạc như địa chỉ nhà hay số điện thoại của Quý khách

Mẹo

myAccess là một hệ thống có độ xác thực thuận tiện và mang tính hiệu quả cao yêu cầu các mật khẩu Quý khách chỉ sử dụng một lần để cho phép các hoạt động và giao dịch myAccess nhất định. Hãy tìm hiểu thêm về dịch vụ miễn phí này và cách nó có thể bảo vệ Quý khách tại myAccess – Bảo mật và An ninh trực tuyến.

Quý khách có thể làm gì để bảo vệ chính mình?

Có những bước quan trọng Quý khách cần thực hiện để bảo vệ chính Quý khách trước các mối đe dọa trực tuyến như chương trình tội phạm tài chính và tội phạm nặc danh. Việc áp dụng các bước dưới đây để bảo vệ máy tính của Quý khách không chỉ giúp tiết kiệm thời gian của Quý khách và tránh những phiền phức nếu có xảy ra mà còn bảo đảm Quý khách sẽ có được kinh nghiệm sử dụng mạng tốt nhất.

Ứng dụng an ninh mạng

Mỗi một máy tính dùng để truy cập vào dịch vụ Ngân hàng trực tuyến cần cài một ứng dụng an ninh mạng để bảo vệ Quý khách trước các chương trình tội phạm tài chính và bảo vệ nhận dạng trực tuyến của Quý khách. Ứng dụng an ninh mạng từ một nhà cung cấp uy tín phải bao gồm:

- Chống vi rút – ngăn chặn chương trình tội phạm tài chính không làm hại máy tính của Quý khách
- Chống gián điệp mạng – bảo vệ máy tính của Quý khách trước chương trình tội phạm có thể đang cố theo dõi những gì Quý khách thao tác trên mạng.
- Tường lửa – theo dõi các thông tin đang ra vào máy tính của Quý khách để chặn truy cập trái phép.

Cần đảm bảo Ứng dụng An ninh Mạng được đặt chế độ tự động tải các bản cập nhật chống vi-rút hàng ngày nhằm bảo đảm Quý khách được bảo vệ trước các mối đe dọa mới nhất.

Nâng cấp Hệ điều hành của Quý khách

Đảm bảo hệ điều hành của Quý khách luôn được cập nhật là một bước quan trọng trong bảo vệ máy tính của Quý khách. Cả Microsoft và Apple đều thường xuyên phát hành các bản cập nhật hay bản

sửa cung cấp cho Quý khách các tính năng mới và bảo vệ Quý khách trước các loại chương trình tội phạm mới.

Microsoft Windows – dùng bản cập nhật Windows tại địa chỉ http://windowsupdate.microsoft.com/

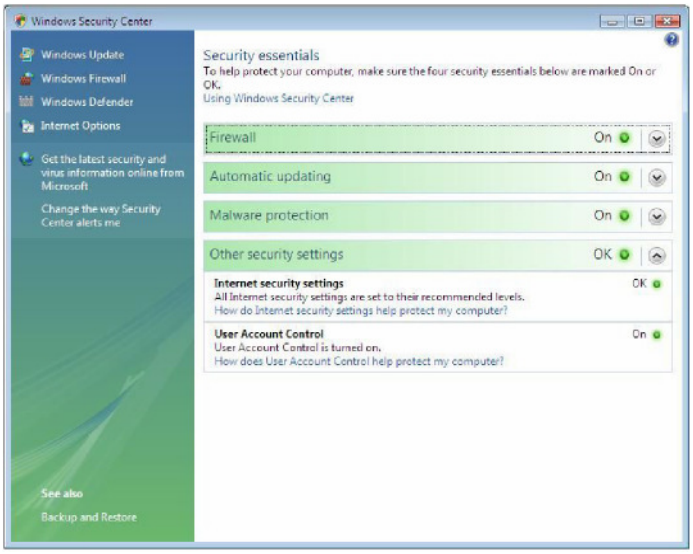
Apple Mac OS X – dùng 'Cập nhật phần mềm' trong Finder

Các bản cập nhật thường được phát hành hàng tháng nhưng có thể có các bản bổ sung an ninh khẩn cấp trong tháng. Quý khách có thể thiết lập cấu hình máy tính của Quý khách để tự động tải xuống và cài đặt các bản cập nhật này.

Trung tâm An ninh Windows

Đối với những người sử dụng hệ điều hành Microsoft Windows, Trung tâm An ninh có thể giúp các Quý khách kiểm soát an ninh trên máy tính của Quý khách bằng cách hiển thị tất cả các chế độ cài đặt về an ninh trên một màn hình thuận tiện. Nó sẽ cảnh báo Quý khách khi phần mềm an ninh hết hạn hoặc khi các thiết lập an ninh cần được củng cố, bảo đảm máy tính của Quý khách được cài đặt để sử dụng myAccess và Internet một cách an toàn.

Minh họa dưới đây cho thấy một chương trình chống virut chưa được cài đặt và cung cấp một đương link '**Tìm một chương trình**' để khắc phục vấn đề an ninh này.



Quý khách có thể vào Trung tâm An ninh Windows bằng cách nhấp chuột vào **Start > Control Panel > Security Center.**