

internet Banking

Tiếp cận không giới hạn

BẢO MẬT TRỰC TUYẾN

- Bảo vệ thông tin của Quý khách hàng
- Các mẹo cần biết
- Thoát khỏi hệ thống InternetBanking khi không sử dụng
- Liên lạc với Sacombank
- Cảnh báo các rủi ro khác
- Một số lời khuyên từ Sacombank về phần mềm cài đặt
- Hệ thống Sacombank hiện đang cung cấp giải pháp bảo mật an toàn sau cho Quý khách

Nhằm đảm bảo duy trì tính bảo mật và an toàn cao nhất cho trang web và cho Quý khách hàng sử dụng InternetBanking, Sacombank khuyến khích Quý khách hàng đọc và nắm rõ những thông tin dưới đây:

Bảo vệ thông tin của Quý khách hàng: Cách đặt và bảo mật mật khẩu

Quý khách hàng vui lòng thực hiện theo các lời khuyên dưới đây của Sacombank nhằm tránh những rủi ro không đáng có có thể xảy ra:

Cách đặt mật khẩu:

- » Chọn một mật khẩu tốt là mật khẩu phải tích hợp chữ hoa, chữ thường, số và các kí tự đặc biệt.
- » Mật khẩu nên có độ dài từ 8 kí tự trở lên.
- » Tránh đặt mật khẩu như tên của Quý khách hàng hoặc số điện thoại, ngày sinh nhật... và các thông tin cá nhân khác dùng làm mật khẩu hoặc những từ ngữ có trong từ điển.



Cách bảo mật mật khẩu:

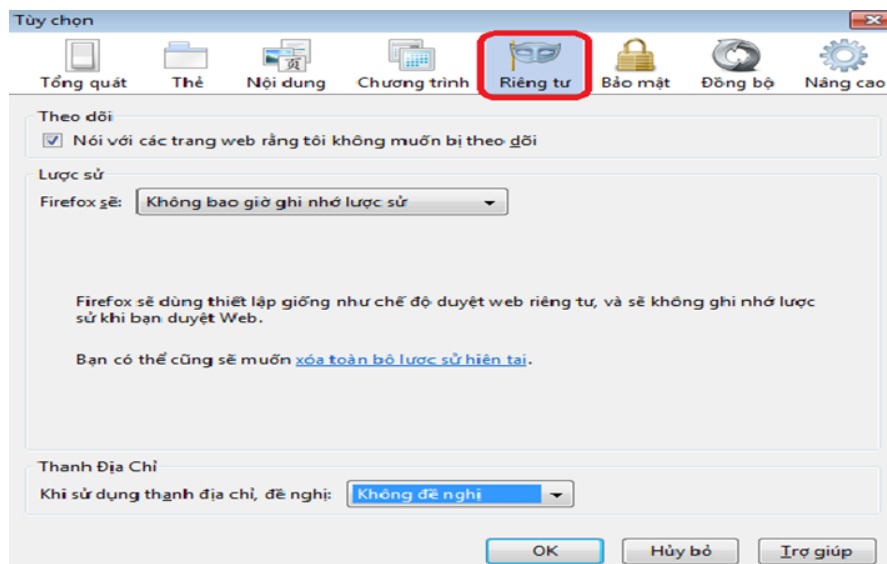
- » Quý khách hàng tự bảo quản thông tin tên đăng nhập, mật khẩu và số định danh của mình, không nên để lộ thông tin cho người khác biết.
- » Thường xuyên thay đổi mật khẩu và số định danh.
- » Không viết mật khẩu ra giấy.
- » Không chia sẻ mật khẩu với người khác.
- » Tránh dùng mật khẩu giống nhau cho các dịch vụ khác nhau.
- » Sau khi thực hiện giao dịch nên thoát khỏi website bằng cách nhấn nút “Thoát” trên trình duyệt.
- » Không thực hiện chức năng tự sao lưu thông tin đăng nhập trên máy.
- » Thông báo ngay với Sacombank nếu quý khách biết rằng mật khẩu của mình đã bị lộ hoặc bị người khác sử dụng.

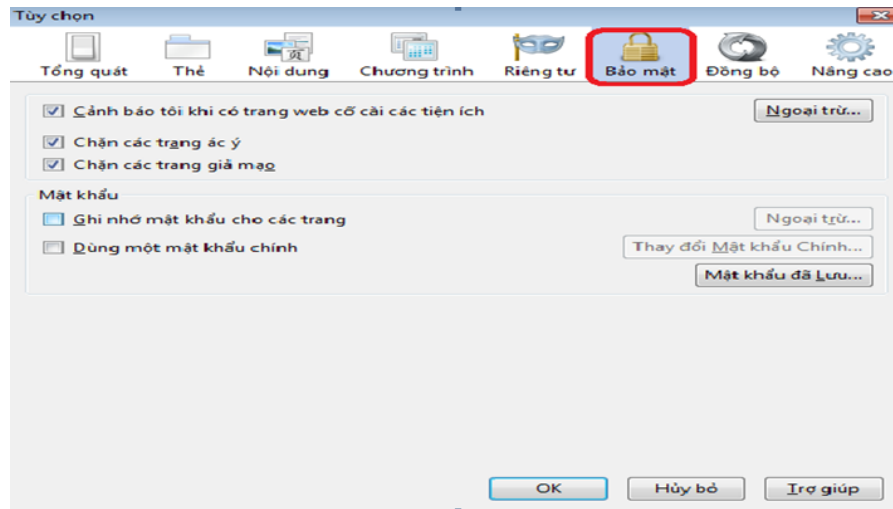
Các mẹo cần biết:

Không đặt tùy chọn của trình duyệt web cho phép lưu lại tên và mật khẩu người dùng

Khi sử dụng một số trình duyệt web thông dụng như Internet Explore hay Firefox khách hàng không nên lưu lại các thông tin như tên website truy cập và tự động chọn chế độ lưu mật khẩu. Khách hàng cũng nên bật các tính năng bảo mật của trình duyệt lên như:

- » **Đối với trình duyệt Firefox** trên thanh công cụ của trình duyệt Quý khách hàng chọn tab (**Công cụ -----> Tùy chọn**) và làm theo hướng dẫn bên dưới :





- » **Đối với trình duyệt Internet Explore** trên thanh công cụ của trình duyệt Quý khách hàng chọn tab (Tools ----> Delete Browsing History)

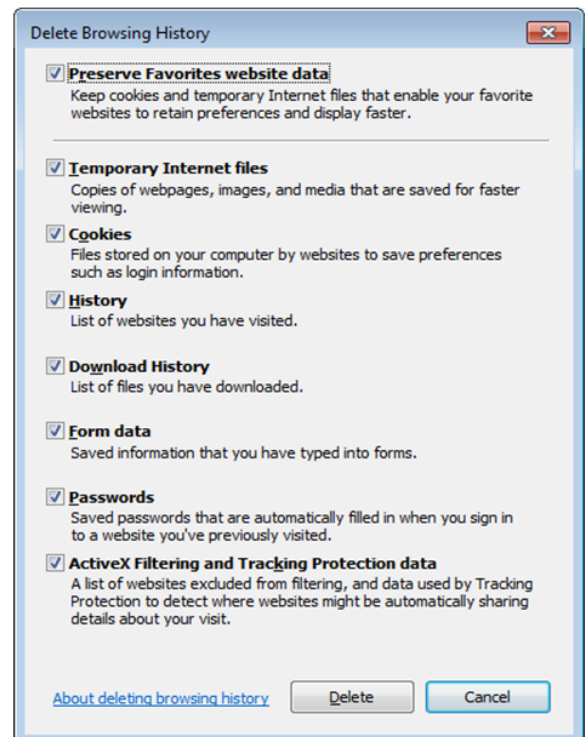
Thoát khỏi hệ thống InternetBanking khi không sử dụng

Khi không sử dụng hoặc rời khỏi máy Quý khách hàng nên khóa máy và thoát khỏi trang giao dịch mà mình đang thực hiện bằng cách click chuột vào mục THOÁT trên trình duyệt.

- » Luôn gõ địa chỉ website của ngân hàng mà Quý khách hàng thực hiện giao dịch vào thanh địa chỉ của trình duyệt web: <https://www.e-sacombank.com.vn>
- » Quý khách hàng không nên đăng nhập thông tin tài khoản của mình từ một liên kết nào đó và từ đây sẽ kết nối đến ngân hàng.
- » Thận trọng, hạn chế dùng máy tính công cộng, mạng không dây công cộng để truy cập vào hệ thống InternetBanking (Café Wifi, trung tâm mua sắm, siêu thị, nhà sách...) vì môi trường này là không an toàn và khách hàng có thể bị đánh cắp các thông tin nhạy cảm của mình như: Mã Pin, Username , Password...
- » Bảo vệ máy tính của Quý khách không bị nhiễm virus bằng cách sử dụng phần mềm diệt virus và được cập nhật liên tục từ nhà cung cấp.
- » Sử dụng bức tường ng lửa cá nhân (Personal Firewall) làm vách ngăn bảo vệ giữa máy tính Quý khách hàng và hệ thống internet.
- » Phải thận trọng. Không mở các email có file đính kèm được gửi từ những nguồn lạ.

Liên lạc với Sacombank ngay khi:

- » Quý khách gặp các lỗi và sự cố trong quá trình sử dụng dịch vụ theo thông tin liên hệ sau:
- » Trung tâm dịch vụ khách hàng Sacombank (TTDVKH): phục vụ 24/7– Tel: 1900 5555 88 hoặc gửi Email về: ask@sacombank.com
- » Khi Quý khách sử dụng InternetBanking với phương thức xác thực qua SMS -> khi bị mất điện thoại hoặc sử dụng loại hình xác thực qua Token -> khi bị mất Token, Quý khách hàng vui lòng liên hệ Trung Tâm Dịch Vụ Khách Hàng Sacombank qua tổng đài 1900 5555 88 hoặc đến điểm giao dịch Sacombank gần nhất để thông báo và yêu cầu khoá hiệu lực của loại hình xác thực của quý khách.



- » Liên hệ ngay với Sacombank nếu Quý khách nhận được một thư điện tử khả nghi hoặc một cuộc điện thoại từ một người nào đó mà khách hàng không rõ và yêu cầu Quý khách nhập các thông tin đăng nhập của Quý khách. Quý khách **KHÔNG ĐƯỢC** thực hiện theo yêu cầu đó thậm chí nếu yêu cầu đó có vẻ như là từ phía Sacombank vì ngân hàng Sacombank sẽ không bao giờ yêu cầu Quý khách tiết lộ mật khẩu, số PIN hay Mã Bảo mật thông qua điện thoại hoặc thư điện tử.

Cảnh báo các rủi ro khác:

Sau đây là một số ví dụ điển hình về các mối nguy mà Quý khách hàng có thể gặp phải khi sử dụng internet để thực hiện giao dịch trực tuyến :

- » Virus & Worms: Là mã chương trình mà nó tự tái tạo hoặc gửi đi trên internet nhằm tàn phá dữ liệu của máy tính hoặc làm gián đoạn hoạt động của hệ thống.
- » Trojans: Là một chương trình gián điệp lây nhiễm vào máy tính của Quý khách hàng mà Quý khách hàng không nhận biết. Nó có thể thực hiện đánh cắp các thông tin nhạy cảm của Quý khách hàng.
- » Phishing: Sử dụng một tên sai như một website giả mạo để đánh lừa khách hàng đăng nhập vào.
- » Pharming: Làm chuyển hướng kết nối của khách hàng đến một máy chủ giả mạo.
- » Rootkit: Là một phần mềm xấu nó cho phép truy cập không xác thực với quyền quản trị trên hệ thống và thực hiện các hành vi bất hợp pháp trên máy tính Quý khách hàng
- » Hacking: Truy cập bất hợp pháp vào máy tính khách hàng bằng internet.

Một số lời khuyên từ Sacombank về phần mềm cài đặt

Để an toàn trong việc thực hiện các giao dịch trực tuyến với Ngân Hàng, Quý khách hàng cần:

- » **Đảm bảo rằng trên máy tính của Quý khách hàng có các chương trình vá lỗi và được cập nhật bản mới nhất từ nhà cung cấp.**

Một trong những điểm yếu dễ bị khai thác nhất đó là phần mềm bị lỗi hỏng chưa được vá lỗi trên máy tính của Quý khách hàng. Và với điểm yếu này, kẻ xấu sẽ dễ dàng lợi dụng để khai thác và lấy đi các thông tin, dữ liệu nhạy cảm từ Quý khách hàng.

Chính vì điều này mà Quý khách hàng phải thường xuyên cập nhật các bản vá lỗi từ nhà cung cấp. Người dùng sử dụng hệ điều hành nào hoặc phần mềm do nhà cung cấp nào thì nên vào trực tiếp website của nhà cung cấp đó để tải về những phiên bản mới nhất có thể.

- » **Cài đặt chương trình chống virus, malware, rootkit**

Khách hàng nên cài đặt thêm một số chương trình an ninh trên máy tính của mình vì một số vấn đề về an toàn bảo mật không thể đảm bảo bởi một hệ điều hành trên máy tính cá nhân. Vì vậy một trong những vấn đề quan trọng là phải có một chương trình quét virus hiệu quả và được cập nhật liên tục từ nhà cung cấp để đảm bảo chương trình có khả năng phát hiện và ngăn chặn những loại virus mới nhất

Máy tính cá nhân rất dễ bị nhiễm các loại Virus, malware, spyware, rootkit từ môi trường internet nếu trên máy tính của Quý khách hàng không được cài đặt các chương trình phòng chống virus một cách hiệu quả. Vì vậy khách hàng nên cài đặt các phiên bản thương mại của các hãng có uy tín trong lĩnh vực này như: Symantec, Kaspersky McAfee, AVG... hoặc có thể sử dụng phần mềm miễn phí của Microsoft "Microsoft Security Essentials" . Khách hàng có thể tải trực tiếp từ website của Microsoft.com

- » **Sử dụng bức tường lửa cá nhân, chương trình dò tìm và phát hiện xâm nhập.**

Sử dụng bức tường lửa cá nhân và các chương trình dò tìm phát hiện xâm nhập trên máy tính Quý khách hàng là một trong những phương thức hiệu quả giúp khách hàng nhận biết và ngăn chặn các cuộc tấn công hoặc truy cập trái phép từ những đối tượng không mong muốn.

Khách hàng có thể sử dụng một số chương trình phổ biến như : Zone Alarm, Patriot

- » **Đảm bảo việc Quý khách hàng truy cập đúng trang web của Ngân Hàng mà khách hàng cần thực hiện giao dịch.**

Việc truy cập không đúng trang web của Ngân hàng mà khách hàng muốn giao dịch. Những kẻ xấu sử dụng một trang web giả mạo giống như trang web thật của Ngân hàng mà khách hàng muốn giao dịch nhằm đánh lừa khách hàng nhập vào các thông tin nhạy cảm của mình vào và lúc đó, các thông tin này sẽ được gửi đến máy của kẻ xấu và kẻ xấu có thể sử dụng thông tin này để thực hiện hành vi gây thiệt hại tài chính hoặc uy tín của Quý khách hàng .

Để khắc phục mối nguy này khách hàng nên thực hiện một số thủ thuật sau:

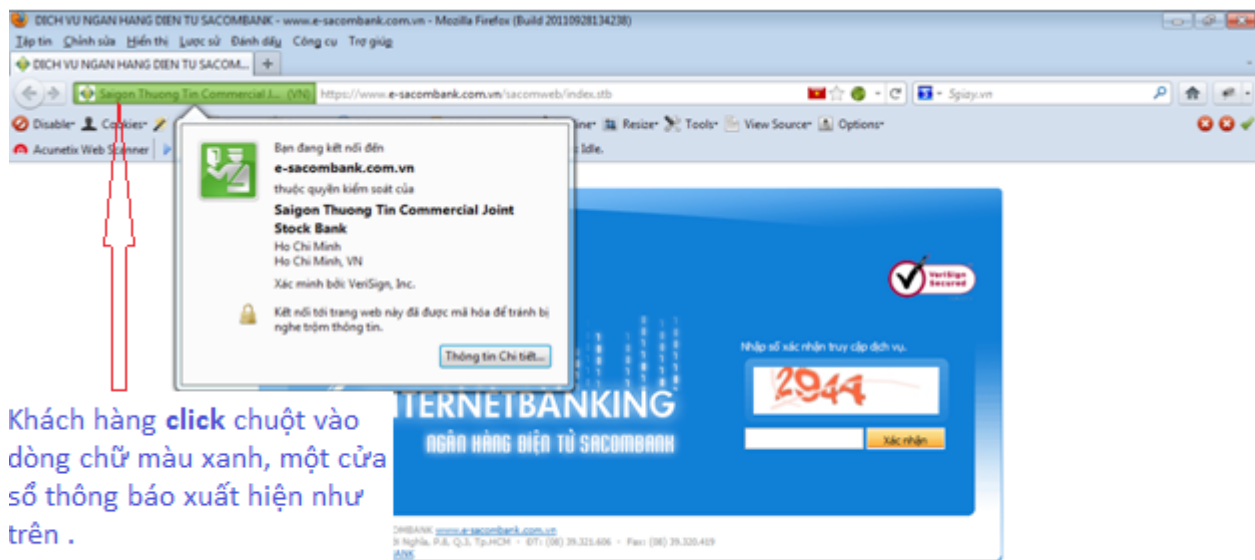
1. Luôn gõ địa chỉ website của ngân hàng mà khách hàng muốn giao dịch vào thanh địa chỉ của trình duyệt web: <https://www.e-sacombank.com.vn>
2. Khách hàng không nên đăng nhập thông tin tài khoản của mình từ một liên kết nào đó và từ đây sẽ kết nối đến ngân hàng.
3. Kiểm tra biểu tượng ổ khóa và chứng nhận của website.
4. Nên thay đổi mật khẩu thường xuyên (Xem mục hướng dẫn cách đặt mật khẩu an toàn và hiệu quả)
5. Hãy liên lạc với Ngân hàng khi khách hàng nhận được cuộc gọi hoặc thư điện tử yêu cầu khách hàng khai các thông tin liên quan đến tài khoản ngân hàng, thay đổi mật khẩu

» Chỉ nên sử dụng những chương trình hợp pháp

Khách hàng không được tải những chương trình trên internet từ những website không hợp pháp hoặc không xác định được nguồn gốc và cài đặt vào máy tính cá nhân của mình
Không được mở những tập tin được gửi từ những email lạ (không rõ người gửi là ai) .
Nên sử dụng chương trình quét virus để quét các tập tin trước khi mở chúng.

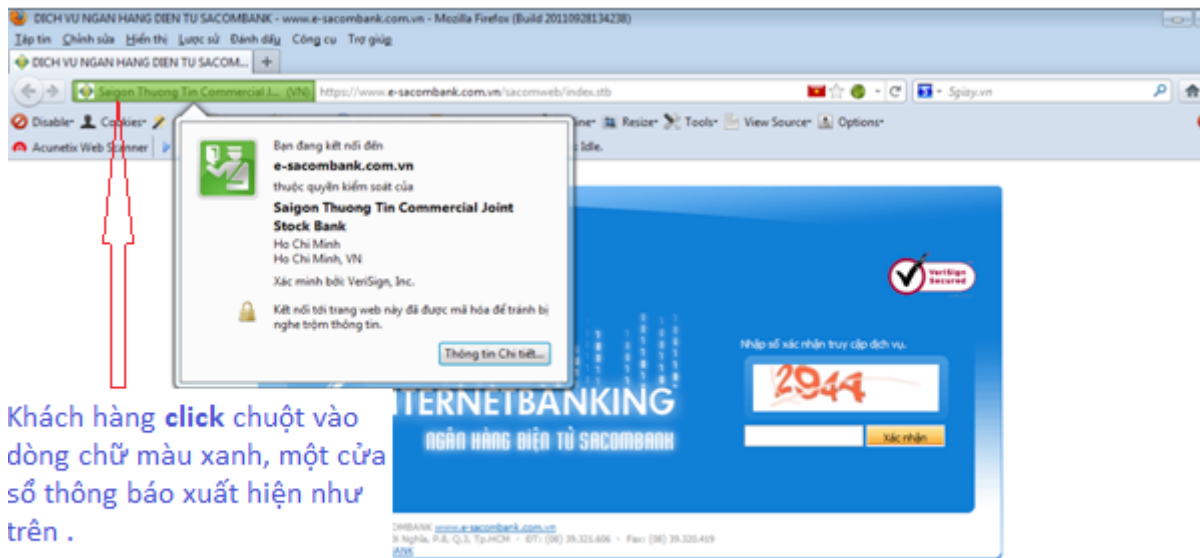
Hệ thống Sacombank hiện đang cung cấp giải pháp bảo mật an toàn sau cho Quý khách:

- » Quý khách đang thực hiện một phiên giao dịch an toàn nếu địa chỉ URL bắt đầu với **https://** hoặc có **biểu tượng ổ khóa xuất hiện tại cửa sổ trình duyệt của Quý khách**.
Bên dưới là trang web thật của Ngân hàng . Khi Quý khách hàng click chuột vào dòng chữ màu xanh trên trình duyệt thì một cửa sổ hiển thị thông tin xuất hiện như bên dưới.



Khách hàng **click** chuột vào dòng chữ màu xanh, một cửa sổ thông báo xuất hiện như trên .

- » Dòng chữ màu xanh trên trình duyệt và thông báo xác nhận rằng website đã được mã hóa bằng giao thức SSL (Secure Sockets Layer) các kết nối tới trang web này đã được mã hóa để tránh bị nghe trộm thông tin và website này thuộc quyền kiểm soát của Ngân Hàng Sài Gòn Thương Tín.
- » Và đây là trang web giả mạo



Khách hàng click chuột vào dòng chữ màu xanh, một cửa sổ thông báo xuất hiện như trên .

Mặc dù trang web cũng được mã hóa bằng giao thức SSL (Secure Sockets Layer), nhưng trên trình duyệt không xuất hiện dòng chữ màu xanh và khi Quý khách hàng click chuột vào cũng không hiện ra bất kì một thông báo nào.

- » **Mã hoá:** Công nghệ mã hoá SSL (Secure Sockets Layer) được sử dụng tại trang web của Ngân hàng để mã hoá (viết mã) các thông tin cá nhân của Quý khách khi Quý khách thực hiện kết nối đến Ngân hàng để thực hiện giao dịch thì các thông tin di chuyển trên đường truyền từ máy tính cá nhân của Quý khách hàng đến Ngân hàng được mã hóa nhằm đảm bảo rằng không một ai khác có thể đọc được thông tin đó.
- » Đây là chứng nhận hợp pháp và sử dụng giao thức mã hóa SSL (Secure Sockets Layer) tại Ngân Hàng Sài Gòn Thương Tín.
- » Nếu Quý khách hàng quên click vào mục “Thoát” trên trình duyệt khi Quý khách đã hoàn tất việc giao dịch của mình với Ngân hàng thì sau một thời gian nhất định kết nối của từ máy tính của Quý khách hàng và Ngân hàng sẽ bị ngắt kết nối. Khi Quý khách hàng muốn thực hiện giao dịch Quý khách hàng phải thực hiện lại việc đăng nhập từ đầu. Điều này nhằm đảm bảo an toàn thông tin cho Quý khách hàng.
- » Việc truy cập vào InternetBanking chỉ được thực hiện khi Quý khách xác thực được với hệ thống chính Quý khách sử dụng khi đăng nhập đúng Tên đăng nhập + Mật khẩu + Số định danh. Ngoài ra một giao dịch chỉ được thực hiện thành công khi Quý khách nhập đúng xác thực cung cấp qua tin nhắn điện thoại hoặc lấy từ Token.
- » Hệ thống tự động khóa thiết bị xác thực Token hoặc không gửi tin nhắn xác thực qua điện thoại di động nếu Quý khách nhập sai mã xác thực quá số lần do Ngân hàng quy định. Để có thể sử dụng lại, Quý khách vui lòng liên hệ với Điểm giao dịch Sacombank gần nhất.

