Sacombank

BẢO MẬT TRỰC TUYẾN

Tại Sacombank, chúng tôi luôn mong muốn đem đến cho khách hàng dịch vụ Ngân Hàng Trực Tuyến tiện lợi và an toàn nhất. Một trong những nỗ lực của chúng tôi nhằm duy trì tính bảo mật cao nhất cho trang web cũng như cho người sử dụng dịch vụ Ngân Hàng Trực Tuyến của chúng tôi. Vì vậy, Ngân hàng khuyến khích Quý khách đọc và nắm rõ những thông tin dưới đây.

Vui lòng liên lạc với chúng tôi trong trường hợp Quý khách không chắc chắn về giá trị pháp lý của bất kỳ yêu cầu nào được cho là từ ngân hàng chúng tôi: Trung tâm dịch vụ khách hàng Sacombank (TTDVKH): phục vụ 24/7– Tel: **1900 5555 88** hoặc gửi Email về: **ask@sacombank.com**

1. BÁO ĐỘNG AN NINH, PHÒNG TRÁNH GIAN LẬN & LỪA ĐẢO TRỰC TUYẾN

Chúng tôi muốn Quý khách quan tâm tới các trang web và thư điện tử được cho là của ngân hàng Sacombank dù là ở Việt Nam hay ở một nơi nào khác. Những trang điện tử và thư điện tử này nhằm mục đích yêu cầu cung cấp thông tin cá nhân nhạy cảm chẳng hạn như: Tên đăng nhập, mật khẩu, câu hỏi bí mật... Một khi có được những thông tin đó, bên giả mạo có thể truy cập được vào tài khoản của người sử dụng, chuyển tiền cho một bên thứ ba, hoặc đóng giả người sử dụng, đấy là mới chỉ kể một số trường hợp.

1.1. Phần mềm và Games không rõ nguồn gốc

- Mô tả:
  Quý khách hàng nhìn thấy một số phần mềm và Games rất tiện ích và hấp dẫn nên đã tải về điện thoại hoặc máy vi tính nhưng không biết rõ nguồn gốc.
  Các chương trình này sau khi được cài đặt thành công sẽ mã hóa điện thoại hoặc máy tính của Quý khách, khi đó toàn bộ thông tin dữ liệu của khách hàng 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 về tài chính hoặc uy tín của Quý khách hàng.
  Ví dụ: trường hợp khách hàng sử dụng chính điện thoại đó để nhận mã xác thực (OTP) thì kẻ xấu sẽ lấy mã xác thực để thực hiện các giao dịch tài chính, …
- Cách khắc phục:
  - » Nên liên lạc ngay với Ngân hàng khi Quý khách nhận mã xác thực OTP mà tại thời điểm đó Quý khách không đăng nhập hay thực hiện bất kỳ giao dịch nào trên kênh eBanking.
  - » Khách hàng không nên tải phần mềm và Games không rõ nguồn gốc

1.2. Điện thoại khách hàng bị cài phần mềm gián điệp

- Mô tả:
  Điện thoại khách hàng có thể bị người quen (vô tình hoặc cố ý) cài đặt phần mềm gián điệp. Khi đó toàn bộ thông tin dữ liệu của Quý khách 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.
  Ví dụ: trường hợp khách hàng sử dụng chính điện thoại đó nhận mã xác thực (OTP) thì kẻ xấu sẽ lấy mã xác thực để thực hiện các giao dịch tài chính, …
- Cách khắc phục:
  - » Nên liên lạc ngay với Ngân hàng khi Quý khách nhận mã xác thực OTP mà tại thời điểm đó chính Quý khách không có đăng nhập hay làm bất kỳ giao dịch nào trên kênh eBanking.
  - » Khách hàng cần bảo quản các thiết bị điện tử cá nhân cẩn thận (ví dụ: không nên cho người khác mượn điện thoại, …)

1.3. Các website giả mạo

- Mô tả:

Sacombank

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 như: tên đăng nhập, mật khẩu đăng nhập, khi đó toàn bộ thông tin của Quý khách 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.

- Cách khắc phục:
  - » Luôn luôn gõ địa chỉ www.isacombank.com.vn; trực tiếp vào thanh địa chỉ của trình duyệt.
  - » Kiểm tra biểu tượng ổ khóa đã khóa và chứng nhận của website trên cửa sổ trình duyệt của Quý khách.
  - » Không đăng nhập thông tin tài khoản của Quý khách từ một liên kết nào đó và từ đây sẽ kết nối đến ngân hàng.
  - » Nên thay đổi mật khẩu thường xuyên (Xem mục hướng dẫn cách đặt mật khẩu an toàn và hiệu quả)
  - » Liên lạc ngay với Ngân hàng khi Quý khách nhận được cuộc gọi hoặc thư điện tử khả nghi yêu cầu Quý khách hàng phải khai báo hoặc tiết lộ các thông tin đăng nhập, tài khoản hay thay đổi mật khẩu… **KHÔNG ĐƯỢC** hành động theo yêu cầu đó thậm chí nếu yêu cầu đó có vẻ như là từ phía ngân hàng 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.

1.4. Thư điện tử (Email) giả mạo:

- Mô tả:

Những kẻ xấu thường mạo danh một tổ chức hợp pháp như ngân hàng, doanh nghiệp… gửi thư điện tử đến Quý khách để:

  - » Yêu cầu cung cấp thông tin mật qua thư điện tử bao gồm: ngày tháng năm sinh, thông tin đăng nhập…
  - » Yêu cầu trả trước một khoản tiền giống như một khoản lệ phí / thuế / hối lộ để được nhận một số tiền lớn hơn, thường là bằng đô la Mỹ
  - » Thông báo rằng Quý khách đã giành được một giải thưởng số xố

Với các hành động tương tự như trên, kẻ xấu thực hiện đều nhằm mục đích là sử dụng thông tin đánh cắp được để làm tổn hại đến tài khoản ngân hàng và danh tiếng của Quý khách.

- Cách khắc phục:
  - » Đừng bao giờ trả lời thư điện tử có yêu cầu cung cấp thông tin cá nhân, hoặc thông tin tài chính và đừng bao giờ nhấp chuột vào liên kết trong thư điện tử đó.
  - » Ngân hàng Sacombank sẽ không bao giờ hỏi các thông tin đăng nhập và các thông tin cá nhân của Quý khách để phục vụ cho các dịch vụ ngân hàng trực tuyến. Những thông tin này bao gồm Mật khẩu, Mã xác thực.
  - » Không được đọc to mật khẩu… trong khi gọi điện thoại, vì không có trung tâm dịch vụ khách hàng nào lại yêu cầu những thông tin đó qua điện thoại cả. Nếu Quý khách quên mật khẩu, thì ngân hàng sẽ hỏi một vài câu hỏi liên quan tới thông tin cá nhân của Quý khách để xác thực chứ không phải hỏi mật khẩu của Quý khách.
  - » Đăng nhập trực tiếp từ trình duyệt của Quý khách. Điều này sẽ tránh cho Quý khách không bị chuyển tới một trang web giả mạo. Nhớ rằng: Thư điện tử do ngân hàng Sacombank gửi sẽ không bao giờ có siêu liên kết tới trang đăng nhập của ngân hàng chúng tôi.
  - » Hãy liên hệ với chúng tôi nếu Quý khách có bất kỳ lo lắng hay nghi nghờ về điều gì được cho là từ phía Ngân hàng chúng tôi.

2. THÔNG TIN BẢO MẬT TRỰC TUYẾN

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:

2.1. Lời khuyên của Sacombank về mật khẩu

- 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 tối thiểu 6 ký tự và tối đa 20 ký tự.
  - » 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.

Sacombank

- Cách bảo mật mật khẩu:
  - » Quý khách hàng tự bảo quản thông tin tên đăng nhập, mật khẩu của mình, không nên để lộ thông tin cho người khác biết.
  - » Thường xuyên thay đổi mật khẩu.
  - » 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 "Đăng xuất" 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.

2.2. Một số lưu ý về trình duyệt sử dụng để giao dịch

Quý khách lưu ý không đặt tùy chọn của trình duyệt web cho phép lưu lại tên và mật khẩu người dung. 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 Firefox phiên bản Tiếng Anh trên thanh công cụ của trình duyệt Quý khách hàng chọn tab (Tools/Options)
- » Đối với trình duyệt Internet Explore trên thanh công cụ của trình duyệt Quý khách hàng chọn tab (Tools/Delete Browsing History)

2.3. Thoát khỏi hệ thống iBanking khi không sử dụng

"Đăng xuất" khỏi hệ thống iBanking khi không sử dụng, vui lòng thực hiện các bước sau:

- » 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 Đăng xuất trên trình duyệt.
- » 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 Internet-Banking (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 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.

2.4. Cài đặt và cập nhật một số phần mềm

- Cập nhật phần mềm:
  - » 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 lỗ hổng 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.

Sacombank

- 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 để 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 Secrity 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…

2.5. 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 diệp lây nhiễm vào máy tính của Quý khách hàng mà Quý khách hàng không nhận biết. Nó có thể thực hiện viện 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.

3. TRÁCH NHIỆM CỦA QUÝ KHÁCH

- » Bảo mật thông tin tài khoản của Quý khách, nghĩa là không công khai những thông tin đó
- » Không bao giờ viết những thông tin bảo mật hoặc tiết lộ chúng cho bất kỳ ai
- » Truy cập tài khoản của Quý khách tại các địa điểm riêng tư ví dụ nhà riêng, văn phòng
- » Thường xuyên đổi mật khẩu
- » Đăng xuất hợp lệ bằng cách sử dụng nút «Đăng xuất» khi phiên giao dịch ngân hàng điện tử của Quý khách kết thúc
- » Luôn ngừng kết nối Internet khi Quý khách kết thúc giao dịch, không bao giờ để máy tính kết nối mạng khi Quý khách không sử dụng dịch vụ nữa
- » 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).
- » Cài đặt bức tường lửa cá nhân và phần mềm phát hiện vi rút trên các máy tính cá nhân và cập nhật các chương trình đó thường xuyên để đảm bảo máy tính được bảo vệ.

4. TRÁCH NHIỆM CỦA SACOMBANK

Chúng tôi bảo vệ Quý khách giao dịch trực tuyến một cách an toàn và bảo mật, bằng cách:

Sacombank

- Tạo ra các phiên giao dịch an toàn: Quý khách đang thực hiện một phiên giao dịch an toàn nếu địa chỉ URL bắt đầu với **https://** và có biểu tượng **ổ khoá** xuất hiện tại cửa sổ trình duyệt. Bên dưới là trang web thật của Ngân hàng. Khi Quý khách hàng bấm chuột vào dòng chữ màu xanh trên trình duyệt thì một cửa sổ hiển thị thông tin xuất hiện như bên dưới.
- Sử dụng mã hoá: Công nghệ mã hoá SSL (Secure Sockets Layer) được sử 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. Sacombank cũng sử dụng giao thức mã hóa SSL (Secure Sockets Layer) để bảo vệ Quý khách.
- Cài đặt thời gian tạm ngưng phiên giao dịch: Nếu Quý khách hàng quên đăng xuất sau khi thực hiện giao dịch ngân hàng trực tuyến thì sau một khoảng thời gian nhất định, kết nối 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 đảo bảo an toàn thông tin cho Quý khách hàng.
- Sử dụng tên đăng nhập và mật khẩu để đảm bảo rằng chúng tôi đang giao dịch với Quý khách: Việc truy cập vào iBanking 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. Vì lý do này, Quý khách không được cho người khác biết mật khẩu của mình và không được dùng một mật khẩu cho các dịch vụ khác nhau.
- Sử dụng hai tầng xác thực để cung cấp thêm một lớp bảo vệ: Ngoài việc nhập đúng tên đăng nhập và mật khẩu thì để thực hiện một giao dịch thành công, Quý khách cần phải nhập đúng MÃ XÁC THỰC cung cấp qua tin nhắn điện thoại hoặc lấy từ Token. Với công nghệ này, Quý khách có thể tận hưởng các dịch vụ ngân hàng trực tuyến an toàn hơn và đó là một trong những thiết bị nhỏ nhất và dễ sử dụng nhất.
- Sử dụng chương trình tự động khóa thiết bị xác thực Token hoặc không gửi tin nhắn xác thực qua điện thoại di động: 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 Trung Tâm Dịch Vụ Khách hàng Sacombank qua tổng đài 1900 5555 88 hoặc đến điểm giao dịch Sacombank gần nhất.
- Sử dụng chương trình tự động khóa tài khoản: Sau năm lần không đăng nhập thành công, chúng tôi sẽ ngừng việc truy cập trực tuyến vào tài khoản của Quý khách. Để kích hoạt lại tài khoản của mình, Quý khách cần liên hệ liên hệ Trung Tâm Dịch Vụ Khách hàng Sacombank qua tổng đài 1900 5555 88 hoặc đến điểm giao dịch Sacombank gần nhất.