DONGA Bank

CẨM NANG GIAO DỊCH AN TOÀN TRÊN DONGA EBANKING

MỤC LỤC

1. CÁCH THIẾT LẬP MẬT MÃ VÀ BẢO QUẢN THÔNG TIN

1.1 Thiết lập mật mã an toàn

- Mật mã bắt buộc có độ dài tối thiểu 8 ký tự số và tối đa 16 ký tự số.

- Tránh đặt mật mã là số điện thoại, ngày sinh nhật, bản số xe, các dãy số liên tục như 123456 … và các thông tin khác của cá nhân, cũng như các thông tin của người thân dùng làm mật mã hoặc những số, cụm số có trong từ điển.

- Thay đổi mật mã của tài khoản truy cập định kỳ 90 ngày/lần hoặc khi bị lộ, nghi bị lộ hoặc sau khi truy cập sử dụng Internet Banking tại máy tính công cộng.

1.2 Bảo quản thông tin đăng nhập

- Quý khách tự bảo quản thông tin mã số khách hàng, mật mã của mình không nên để lộ hoặc chia sẻ thông tin cho người khác.

- Không viết mật mã ra giấy.

- Tránh dùng mật mã giống nhau cho các dịch vụ khác nhau.

- Thay đổi mật mã truy cập DongA eBanking ngay khi phát hiện ra Quý khách vừa click vào đường link nghi ngờ giả mạo hoặc vô tình trả lời hoặc cung cấp thông tin đăng nhập cho người lạ.

- Không sử dụng các chương trình lưu mã số khách hàng và mật mã hoặc các thông tin đăng nhập khác trên máy tính/ smartphone/ tablet.

- Bảo vệ, giữ bí mật mật mã, thẻ xác thực, mã xác thực qua điện thoại (OTP SMS)... và không chia sẻ các thiết bị lưu trữ các thông tin này.

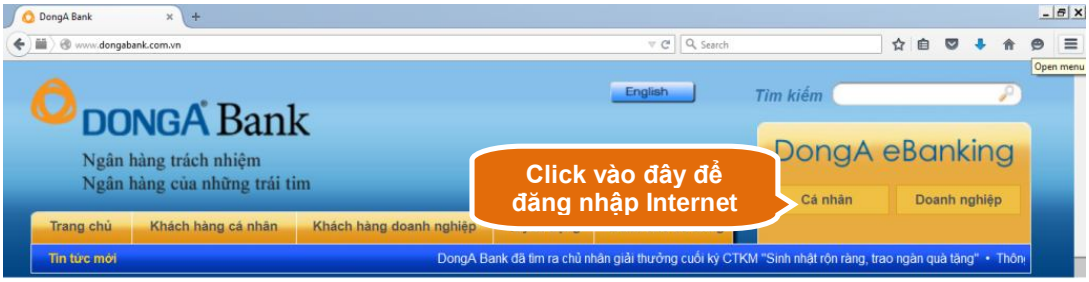
2. ĐĂNG NHẬP, SỬ DỤNG VÀ THOÁT AN TOÀN

2.1 Đăng nhập an toàn

- **(Đề xuất) Luôn luôn** nhập địa chỉ website **https://ebanking.dongabank.com.vn** của DongA Bank vào thanh địa chỉ của trình duyệt web để thực hiện giao dịch.

- Ngoài ra, Quý khách cũng có thể đăng nhập DongA eBanking thông qua các các địa chỉ sau để đảm bảo an toàn.

www.dongabank.com.vn



https://ebanking.dongabank.com.vn/khcn dành cho Khách hàng cá nhân.

https://ebanking.dongabank.com.vn/khdn dành cho Khách hàng doanh nghiệp.

- Đối với Quý khách sử dụng điện thoại thông minh, khi nhập đường link **https://ebanking.dongabank.com.vn** thì trình duyệt của thiết bị sẽ chủ động trả về giao diện dành riêng cho dạng thiết bị này (bên cạnh là hình ảnh minh họa bằng Internet Explore trên Windows Phone 8.1).

- Không đăng nhập thông tin tài khoản của mình từ một liên kết và từ đây sẽ kết nối đến ngân hàng.

- Kiểm tra biểu tượng ổ khóa và chứng nhận của website (xem chi tiết Mục 5.1).

- 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 Quý khách có thể bị đánh cắp các thông tin nhạy cảm của mình như mã PIN, mã số khách hàng, mật mã…

- Chỉ dùng máy tính công cộng để truy cập, thực hiện giao dịch Internet Banking trong trường hợp **thật sự cần thiết** và sau đó phải sử dụng phương tiện an toàn để thay đổi ngay mật mã đăng nhập.

2.2 Sử dụng an toàn

- Đọc kỹ các chính sách của đơn vị chấp nhận thanh toán trước khi đồng ý thanh toán.

- Kiểm tra đầy đủ chính xác các thông tin giao dịch trước khi nhập mã OTP (mã xác thực) để xác nhận giao dịch.

- Chỉ sử dụng thông tin thẻ để thanh toán tại các website uy tín, không nên sử dụng máy tính công cộng thực hiện các giao dịch thanh toán online.

- Khi nhận được tin nhắn OTP từ DongA Bank, cần kiểm tra kỹ nội dung tin nhắn, bao gồm: loại giao dịch, kênh giao dịch... Nếu nội dung tin nhắn không khớp với giao dịch đang thực hiện, Quý khách tuyệt đối không nhập mã OTP vào bất kỳ trang web hoặc tiết lộ cho bất kỳ ai.

- Khi hệ thống đang xử lý giao dịch: Quý khách cần chờ cho đến khi có thông báo kết quả giao dịch từ hệ thống, không thoát khỏi màn hình đang giao dịch để thực hiện giao dịch khác hoặc thoát khỏi hệ thống.

2.3 Thoát an toàn

- "**Thoát**" khỏi hệ thống DongA Internet Banking khi không sử dụng hoặc khi rời khỏi máy tính. Quý khách thoát khỏi trang giao dịch mà mình đang thực hiện bằng cách click chuột vào mục **"Thoát"** trên màn hình (như hình dưới).

- Việc tắt (đóng) tab đang mở Internet Banking của trình duyệt không đồng nghĩa với việc thoát khỏi Internet Banking.

- Tắt hoàn toàn trình duyệt để kết thúc hoàn toàn các phiên giao dịch trên Internet Banking.

- Tắt hoàn toàn trình duyệt hoặc vào lại địa chỉ **https://ebanking.dongabank.com.vn/** để thoát đăng nhập sau khi thực hiện giao dịch thanh toán trực tuyến trước khi rời khỏi máy tính.

3. HƯỚNG DẪN SỬ DỤNG WEBSITE AN TOÀN

- Hạn chế truy cập các website lạ để tránh các mối nguy có thể gặp phải khi sử dụng internet để thực hiện giao dịch trực tuyến:

+ Lừa đảo tài chính: Thường bắt đầu bằng một tin nhắn hoặc email từ một người lạ có hình thức như được gửi trực tiếp tới người nhận để đưa ra đề xuất thực hiện theo yêu cầu từ người gửi, từ đó người nhận sẽ nhận được một khoản tiền lớn nhưng thực tế thì người nhận sẽ không thể nhận được hoặc bị mất tiền/tài sản nếu làm theo yêu cầu.

+ Trộm danh tính: Là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính, chủ yếu là lấy trộm thông tin thẻ tín dụng, tài khoản đăng nhập ebanking để tạo ra một món nợ lớn cho khách hàng hoặc sử dụng tiền trong tài khoản của khách hàng để giao dịch.

+ Phần mềm độc hại (Virus & Worms, Trojans, Phishing, Pharming, Rootkit, Hacking, Keylogger, …): Là bất kỳ loại phần mềm nào được thiết kế để gây hại máy tính hoặc thiết bị di động. Phần mềm độc hại có thể lấy cắp thông tin nhạy cảm từ các thiết bị, làm chậm hoạt động của thiết bị hay thậm chí gửi email giả mạo từ tài khoản email của bạn mà bạn không biết.

- Đảm bảo rằng máy tính hoặc thiết bị di động của Quý khách có các chương trình vá lỗi và được cập nhật bản mới nhất từ nhà cung cấp.

- Bảo vệ máy tính hoặc thiết bị di động không bị nhiễm virus bằng cách sử dụng các phần mềm diệt virus uy tín và được cập nhật liên tục từ nhà cung cấp.

- Bật hoặc sử dụng tường lửa cá nhân (Personal Firewall) làm vách ngăn bảo vệ giữa máy tính hoặc thiết bị di động với hệ thống Internet.

- Phải thận trọng, không mở các email hoặc các file đính kèm được gửi từ những nguồn lạ (không rõ người gửi là ai) hoặc kiểm chứng lại với người gửi để chắc rằng người đó không bị giả mạo. Nên sử dụng chương trình quét virus để quét các tập tin trước khi mở chúng.

- Không trả lời các email có tính chất truy vấn thông tin cá nhân.

- Không cài đặt chế độ trả lời email tự động.

- Không chuyển tiếp (forward) những email có dạng “Hãy gửi email này đến toàn bộ bạn bè của chúng ta”…

- Sử dụng chế độ duyệt web ẩn danh (Private browsing, Lgconito mode, …).

- Thường xuyên xóa lịch sử, cookie, cache sau khi giao dịch trực tuyến.

- Không nên sử dụng các phầm mềm crack, keygen,…

- Không 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 hoặc thiết bị di động.

4. SỬ DỤNG SMARTPHONE AN TOÀN

- Chỉ tải phầm mềm từ các kho lưu trữ chính thống của các hệ điều hành Android (Play Store), iOS (Apple Store), Windows Phone/ Windows Mobile (Microsoft Store).

- Đặt mật khẩu đủ mạnh cho thiết bị di động, để mở khóa sử dụng ứng dụng được cài trên thiết bị.

- Cảnh giác/ không trả lời những câu hỏi yêu cầu thông tin cá nhân hoặc thông tin truy cập dịch vụ, mật khẩu đăng nhập, thông tin tài khoản, thẻ tín dụng từ các nguồn không chính thống.

- Bảo vệ Smartphone của Quý khách không bị nhiễm virus bằng cách sử dụng phần mềm diệt virus uy tín và được cập nhật liên tực từ nhà cung cấp.

- Tắt tính năng cho phép cài đặt các ứng dụng không rõ nguồn gốc "Unknown sources".

- Không sử dụng thiết bị di động đã bị bẻ khóa Jailbreak (iOS) hoặc Root (Android), đặc biệt không sử dụng các thiết bị để cài đặt, đăng nhập sử dụng ứng dụng DongA Internet Banking/ Mobile Banking.

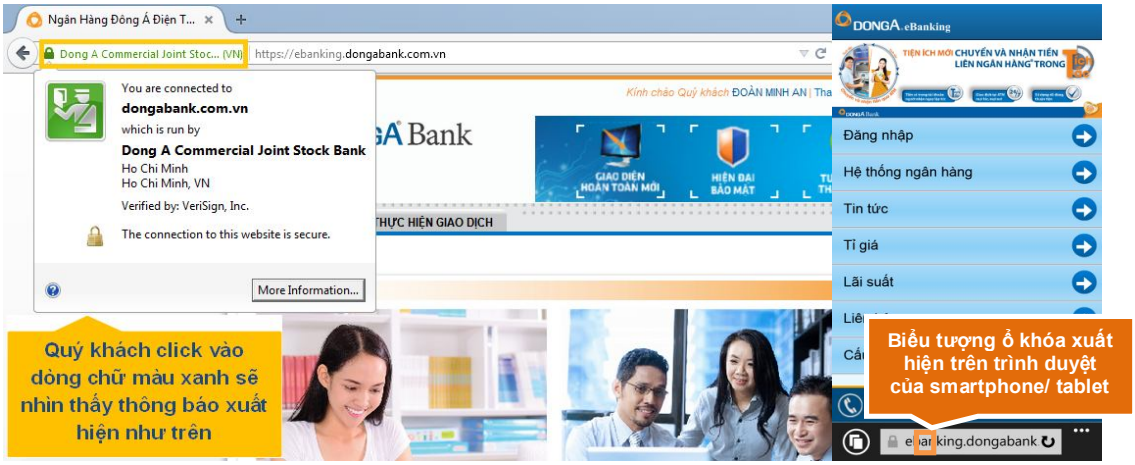
- Cập nhật bản vá mới nhất cho hệ điều hành của điện thoại.

5. GIỚI THIỆU CÁC GIẢI PHÁP AN TOÀN DONGA BANK ĐANG CUNG CẤP ĐỐI VỚI DỊCH VỤ DONGA EBANKING

5.1 Công nghệ mã hoá SSL (Secure Sockets Layer)

- Quý khách đang thực hiện một phiên giao dịch an toàn nếu địa chỉ URL bắt đầu với **https://** hoặc có biểu tượng ổ khoá xuất hiện tại cửa sổ trình duyệt của Quý khách. Bên dưới là trang web thật của Ngân hàng.

- **Đối với máy tính:** Khi Quý khách click chuột vào dòng chữ màu xanh trên trình duyệt thì một cửa sổ hiển thị thông tin xuất hiện như hình bên dưới.
- **Đối với thiết bị di động là Smartphone/ Tablet:** Chỉ có thiết bị chạy hệ điều hành iOS sẽ có dòng chữ màu xanh trên trình duyệt. Các dòng thiết bị chạy hệ điều hành Android và Window Phone chỉ xuất hiện ổ khóa như hình bên dưới.

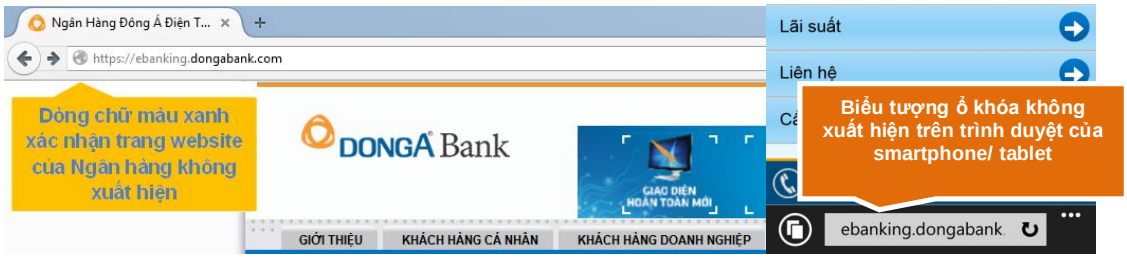


- Dòng chữ màu xanh trên trình duyệt xuất hiện có nghĩa là website đã được mã hóa bằng giao thức SSL, các kết nối tới trang web này đã được mã hóa để tránh bị nghe trộm thông tin và website này thuộc quyền kiểm soát của Ngân hàng TMCP Đông Á.

- Về công nghệ mã hoá SSL được sử dụng tại trang web của Ngân hàng để mã hoá các thông tin cá nhân của Quý khách khi thực hiện kết nối đến Ngân hàng để thực hiện giao dịch, các thông tin được truyền từ thiết bị cá nhân của Quý khách đến Ngân hàng sẽ 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 tại DongA Bank.

Dưới đây là trang web giả mạo



- Mặc dù trang web cũng được mã hóa bằng giao thức SSL nhưng trên trình duyệt không xuất hiện dòng chữ màu xanh và click chuột vào cũng không hiện ra bất kì một thông báo nào.

5.2 Ngắt kết nối sau một thời gian ngưng giao dịch

Trường hợp Quý khách không thực hiện đăng xuất như hướng dẫn tại Mục 2.3 sau khi giao dịch với Ngân hàng thì sau một thời gian nhất định, Ngân hàng sẽ tự ngắt việc đăng nhập của Quý khách để đảm bảo an toàn. Khi muốn thực hiện lại giao dịch mới, Quý khách phải thực hiện đăng nhập từ đầu.

5.3 Yêu cầu đăng nhập đúng mã số khách hàng và mật mã

- Việc truy cập vào DongA eBanking chỉ được thành công khi Quý khách sử dụng đúng Mã khách hàng và Mật mã.

- Một giao dịch tài chính chỉ được thực hiện thành công khi Quý khách nhập đúng mã xác thực được Ngân hàng cung cấp qua tin nhắn điện thoại hoặc Thẻ xác thực hoặc hình thức xác thực khác của DongA Bank.

5.4 Bắt buộc dùng bàn phím ảo để nhập mật mã

Loại bàn phím ảo này giúp hạn chế người khác theo dõi thao tác của Quý khách khi đăng nhập bằng bàn phím vật lý (trong trường hợp máy tính của Quý khách đang bị bí mật theo dõi bằng chương trình keylogger).

5.5 Tự động thay đổi mã xác thực

Hệ thống sẽ tự động hủy hiệu lực mã xác thực của Quý khách trong các trường hợp sau:

- Quá thời gian nhập mã xác thực giao dịch theo quy định.

- Nhập sai mã xác thực 3 lần cho 1 lần giao dịch.

6. LIÊN HỆ VỚI DONGA BANK

Quý khách cần liên hệ ngay đến DongA Bank khi gặp các trường hợp sau:

- Thông báo và yêu cầu khoá hiệu lực của loại hình xác thực đang sử dụng khi phát hiện bị mất điện thoại (nếu sử dụng loại hình xác thực qua SMS) hoặc mất Thẻ xác thực (nếu sử dụng loại hình xác thực qua ma trận) hoặc hình thức xác thực khác.

- Khi phát hiện tài khoản có dấu hiệu bất thường như bị trừ tiền hay nhận được tin nhắn cung cấp mã xác thực nhưng bản thân không thực hiện giao dịch đó.

- Liên hệ và kiểm chứng thông tin khi nhận được yêu cầu cung cấp thông tin đăng nhập như mã khách hàng, mật mã, mã xác thực từ bất kỳ người nào qua bất kỳ hình thức nào.

- Thông tin liên hệ:

- Trung tâm dịch vụ khách hàng của DongA Bank (TTDVKH): phục vụ 24/7– Tel: 1900545464 hoặc gửi Email về: **1900545464@dongabank.com.vn**
- Mạng lưới Chi nhánh/ Phòng giao dịch trên toàn hệ thống DongA Bank (**www.dongabank.com.vn/mang-luoi**).