CẨM NANG GIAO DỊCH AN TOÀN TRÊN NGÂN HÀNG ĐỒNG Á ĐIỆN TỬ

1. Thiết lập mật mã an toàn và bảo quản thông tin đăng nhập

1.1. Thiết lập mật mã an toàn

- **Đặt mật mã** có độ dài theo đúng quy định của dịch vụ Ngân hàng Đông Á điện tử được DongA Bank công bố chính thức theo từng thời kỳ.
- **Không đặt mật mã** là số điện thoại, ngày sinh nhật, biển số xe, các ký tự trùng nhau hoặc liên tục theo thứ tự trong bảng chữ cái, chữ số như abcdef, 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 dịch vụ Ngân hàng Đông Á điện tử định kỳ (tối đa 12 (mười hai) tháng/ lần) hoặc khi bị lộ, nghi bị lộ.

1.2. Bảo quản thông tin đăng nhập

- Tự bảo quản thông tin Mã số khách hàng/ Tên đăng nhập và mật mã, **không để lộ hoặc chia sẻ** thông tin cho người khác.
- **Không dùng mật mã giống nhau** cho các dịch vụ khác nhau.
- Không viết mật mã ra giấy.
- **Không sử dụng các chương trình lưu** Mã số khách hàng/ Tên đăng nhập và mật mã hoặc các thông tin đăng nhập khác trên thiết bị di động/ máy tính.
- Thay đổi mật mã truy cập dịch vụ Ngân hàng Đông Á điện tử ngay khi phát hiện hoặc nghi ngờ vừa truy cập vào đường dẫn giả mạo hoặc vô tình trả lời, cung cấp thông tin tài khoản truy cập dịch vụ Ngân hàng Đông Á điện tử cho người lạ.
- Bảo vệ, giữ bí mật mật mã, thẻ xác thực, mã xác thực OTP, ... và **không chia sẻ các thiết bị lưu trữ** các thông tin này.

2. Hướng dẫn giao dịch an toàn

2.1. Đăng nhập an toàn

- Chỉ dùng Mã số khách hàng/ Tên đăng nhập và mật mã để **đăng nhập trên website Internet Banking chính thức của DongA Bank**: https://ebanking.dongabank.com.vn (hoặc truy cập từ liên kết đặt sẵn có trên website chính thức của DongA Bank là www.dongabank.com.vn), ứng dụng DongA Mobile Internet Banking được cài đặt trên thiết bị di động.
- Đối với giao dịch thanh toán trực tuyến: chỉ thực hiện mua hàng tại những website có

uy tín và mọi đường dẫn đăng nhập Internet Banking của DongA Bank đều phải bắt đầu là https://ebanking.dongabank.com.vn cùng ổ khóa chứng nhận an toàn.

- Đối với thiết bị di động/ máy tính, khi truy cập website Internet Banking 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.

Hình 1. Giao diện Internet Banking trên từng thiết bị

- **Không** nhập thông tin truy cập truy cập dịch vụ Ngân hàng Đông Á điện tử (Mã số khách hàng/ Tên đăng nhập, mật mã, mã xác thực OTP) từ một đường dẫn liên kết và từ đây sẽ kết nối đến Internet Banking của DongA Bank.
- **Không dùng máy tính công cộng** để truy cập, thực hiện giao dịch trên kênh Ngân hàng Đông Á điện tử.
- **Hạn chế dùng mạng Internet không dây** (Wifi) công cộng (quán cà phê, trung tâm mua sắm, siêu thị, nhà sách,…) để truy cập vào Internet Banking, ứng dụng DongA Mobile Internet Banking của DongA Bank, vì môi trường mạng Internet này không an toàn và có thể đánh cắp các thông tin như Mã số khách hàng/ Tên đăng nhập, mật mã, mã xác thực OTP.

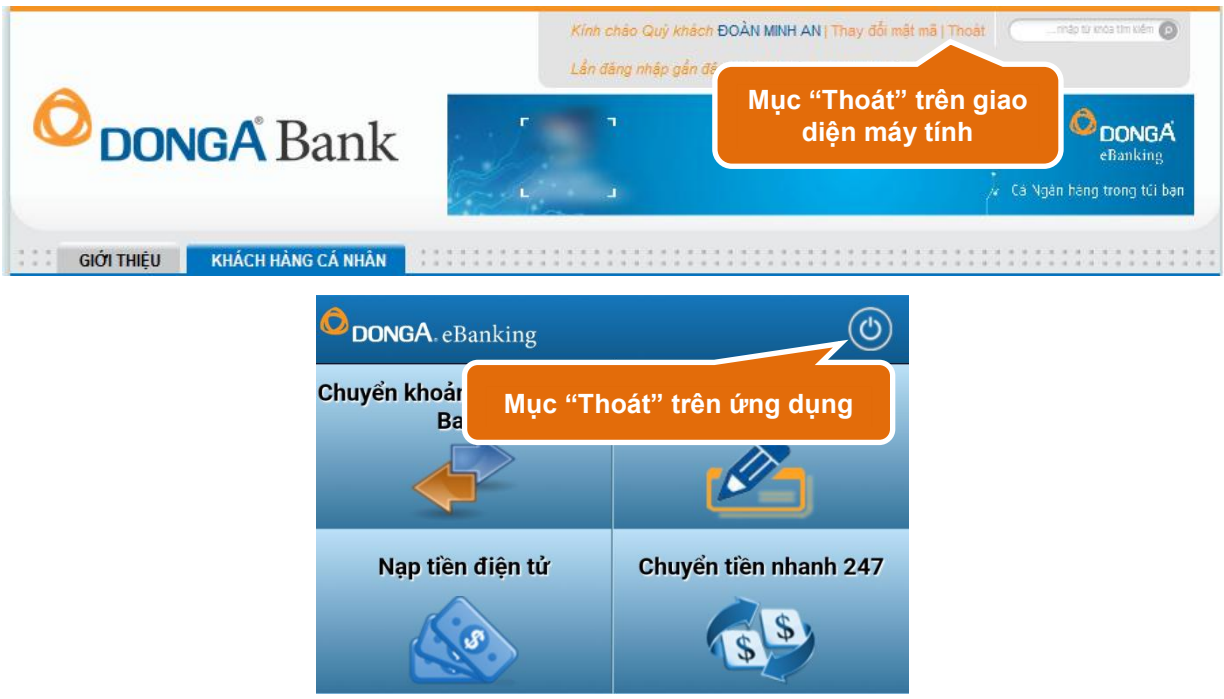
2.2. Thực hiện giao dịch an toàn

- **Đọc kỹ** các chính sách của đơn vị chấp nhận thanh toán trước khi đồng ý thanh toán trực tuyến.
- **Kiểm tra** đầy đủ chính xác các thông tin giao dịch trước khi nhập mã xác thực OTP để xác nhận giao dịch.
- Khi nhận được tin nhắn mã xác thực 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, tuyệt đối không nhập mã xác thực OTP vào bất kỳ website nào hoặc tiết lộ cho bất kỳ ai.
- Khi hệ thống đang xử lý giao dịch, 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 Internet Banking khi không sử dụng, sau khi thanh toán trực tuyến hoặc khi rời khỏi thiết bị đang truy cập Internet Banking bằng cách:
    - **Thoát** khỏi trang giao dịch đang thực hiện bằng cách nhấp vào mục "**Thoát**" trên màn hình.
    - **Tắt trình duyệt** đang truy cập Internet Banking hoặc ứng dụng DongA Mobile Internet Banking để kết thúc hoàn toàn các phiên giao dịch.

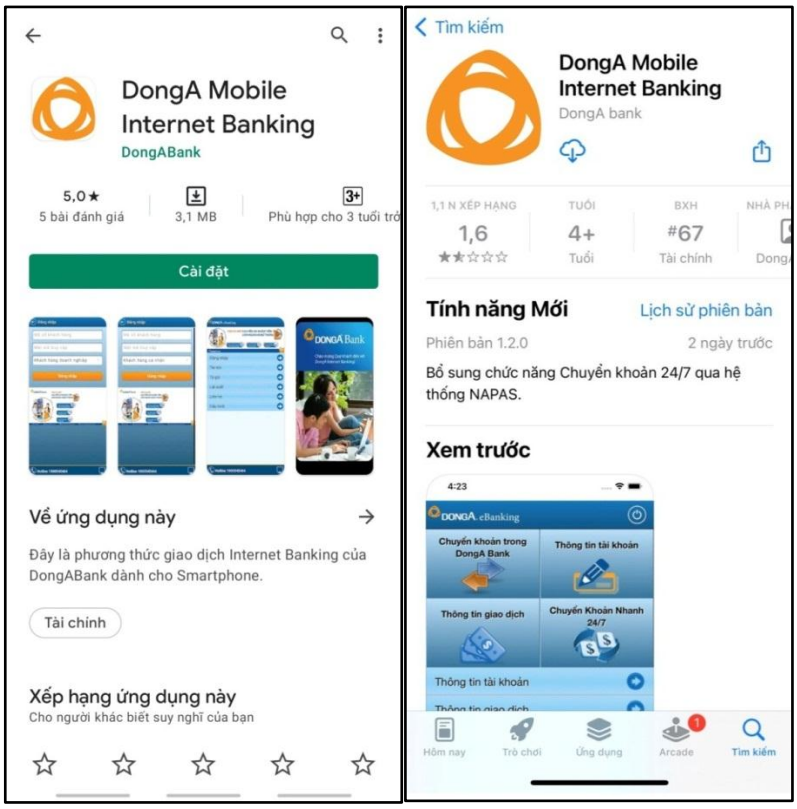


Hình 2. Luôn thoát phiên giao dịch trên Internet Banking khi ngưng sử dụng

- Việc tắt (đóng) thẻ đang mở Internet Banking của trình duyệt không đồng nghĩa với việc thoát khỏi phiên giao dịch.
- 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 màn hình máy tính.

2.4. Sử dụng thiết bị di động/ máy tính an toàn

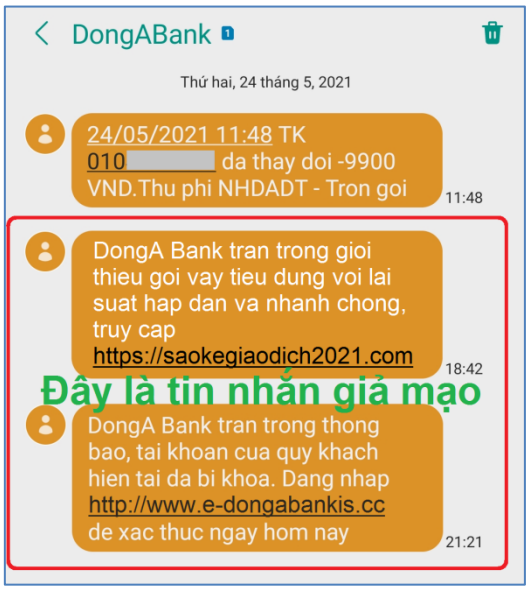
- Đối với ứng dụng DongA Mobile Internet Banking do DongA Bank phát hành tại các cửa hàng ứng dụng, lưu ý chỉ thực hiện cài đặt các ứng dụng có nhà phát hành là **DongA Bank** hoặc **DongABank**, mọi ứng dụng khác có tên tương tự nhưng không phải do DongA Bank phát hành đều là giả mạo.



Hình 3. DongA Mobile Internet Banking trên CH Play và App Store

- **Đặt mật mã/ mật khẩu** đủ mạnh cho thiết bị di động/ máy tính, để mở khóa sử dụng ứng dụng, trình duyệt web được cài trên thiết bị.
- **Cảnh giác/ không trả lời** những câu hỏi yêu cầu cung cấp thông tin cá nhân hoặc thông tin truy cập dịch vụ Ngân hàng Đông Á điện tử, mật mã đăng nhập tài khoản/ dịch vụ Ngân hàng Đông Á điện tử, thông tin của thẻ tín dụng từ các nguồn không chính thống.
- **Bảo vệ thiết bị di động/ máy tính** không bị nhiễm virus, mã độc bằng cách sử dụng phần mềm diệt virus uy tín và được cập nhật liên tục từ nhà cung cấp.
- **Tắt** tính năng cho phép cài đặt các ứng dụng không rõ nguồn gốc vào thiết bị di động.
- Chỉ cài đặt ứng dụng trên cửa hàng ứng dụng CH Play (hệ điều hành Android) và App Store (hệ điều hành iOS). **Không tải, cài đặt** các ứng dụng từ những website không hợp pháp hoặc không xác định được nguồn gốc hoặc từ các đường dẫn không rõ nguồn gốc.
- **Không sử dụng** thiết bị di động đã bị bẻ khóa Jailbreak (đối với hệ điều hành iOS) hoặc Root (đối với hệ điều hành Android), đặc biệt không sử dụng các thiết bị này để cài đặt hay/ và đăng nhập ứng dụng DongA Mobile Internet Banking. Đối với máy tính, không sử dụng, cài đặt các phầm mềm bị bẻ khóa bản quyền sử dụng (phần mềm bẻ khóa crack, keygen,…).
- **Bật hoặc sử dụng tường lửa cá nhân** (Personal Firewall) làm vách ngăn bảo vệ giữa thiết bị di động/ máy tính với hệ thống Internet.

- **Cập nhật** phiên bản mới nhất cho hệ điều hành của thiết bị di động nhằm kịp thời khắc phục các lỗ hổng bảo mật của phiên bản cũ.
- **Nhận biết nội dung tin nhắn** SMS được gửi từ thương hiệu DongA Bank là tiếng Việt không dấu và DongA Bank không bao giờ yêu cầu cung cấp Mã số khách hàng/ Tên đăng nhập, mật mã đăng nhập, mã xác thực OTP, thông tin thẻ tín dụng… trong bất cứ trường hợp nào.



Hình 4. Minh họa về tin nhắn giả mạo được gửi từ Brandname DongA Bank

- **Không** truy cập các website lạ, 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 để tránh các mối nguy có thể gặp phải.
- **Sử dụng** chế độ duyệt website ẩn danh, thường xuyên xóa lịch sử truy cập (cookie, cache) trên trình duyệt sau khi hoàn tất giao dịch trực tuyến.
- **Không** mở các email hoặc các tập tin (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. Sử dụng chương trình quét virus để quét các tập tin trước khi mở chúng.
- **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"…đến email của người khác.
- **Cảnh giác** với việc truy cập bất kỳ liên kết, tập tin đính kèm trong email, tin nhắn SMS hay mạng xã hội, vì đây đều có khả năng là thủ thuật của tin tặc nhằm tấn công vào tài khoản, nhất là đối với các nội dung có chứa yêu cầu cung cấp mật mã, thông tin thẻ ngân hàng, mã xác thực OTP,… Trong bất cứ trường hợp nào cũng nên thực hiện thêm

một thao tác là liên hệ với Tổng đài DongA Bank để được hỗ trợ, xác nhận thông tin.


From: "webmaster" <[redacted]@dongabank.com.vn>
Sent: Thursday, May 28, 2020 3:56:08 AM
Subject: chú ý khẩn cấp

Chúng tôi hiện đang nâng cấp cơ sở dữ liệu và máy chủ email của mình để giảm thư rác và email rác, do đó chúng tôi đang xóa tất cả tài khoản không sử dụng để tạo khoảng trống cho tài khoản mới. Để ngăn chặn tài khoản của bạn bị đóng, bạn phải nhấp vào liên kết bên dưới và đăng nhập để nâng cấp và sao lưu liên lạc và email của bạn tự động.

Nhấn vào đây để xem xét

Điều này là để cải thiện chất lượng dịch vụ của chúng tôi. Chúng tôi xin lỗi vì sự bất tiện này.

Hình 5. Ví dụ về email giả mạo được gửi từ Brandname DongA Bank

2.5. DongA Bank chỉ có **đường dẫn truy cập Internet Banking duy nhất** là https://ebanking.dongabank.com.vn và cũng **không hợp tác với bất kỳ đơn vị nào** hay yêu cầu đăng nhập vào đường dẫn lạ để truy cập vào dịch vụ Ngân hàng Đông Á điện tử, việc đăng nhập tài khoản Internet Banking từ bất kỳ website hoặc ứng dụng nào khác, chính là việc cung cấp thông tin dịch vụ Ngân hàng Đông Á điện tử cho người khác và có nguy cơ xảy ra rủi ro cho tài khoản.

Hình 6. Ví dụ về đường dẫn giả mạo truy cập dịch vụ Ngân hàng Đông Á điện tử

2.6. **Đăng ký dịch vụ** thông báo phát sinh giao dịch để luôn nhận được thông báo từ DongA Bank về những biến động số dư trong tài khoản, từ đó kiểm soát được những giao dịch đáng ngờ.

2.7. Trường hợp nghi ngờ tài khoản bị lộ thông tin hoặc có giao dịch đáng ngờ, có thể chủ động thực hiện các cách sau:

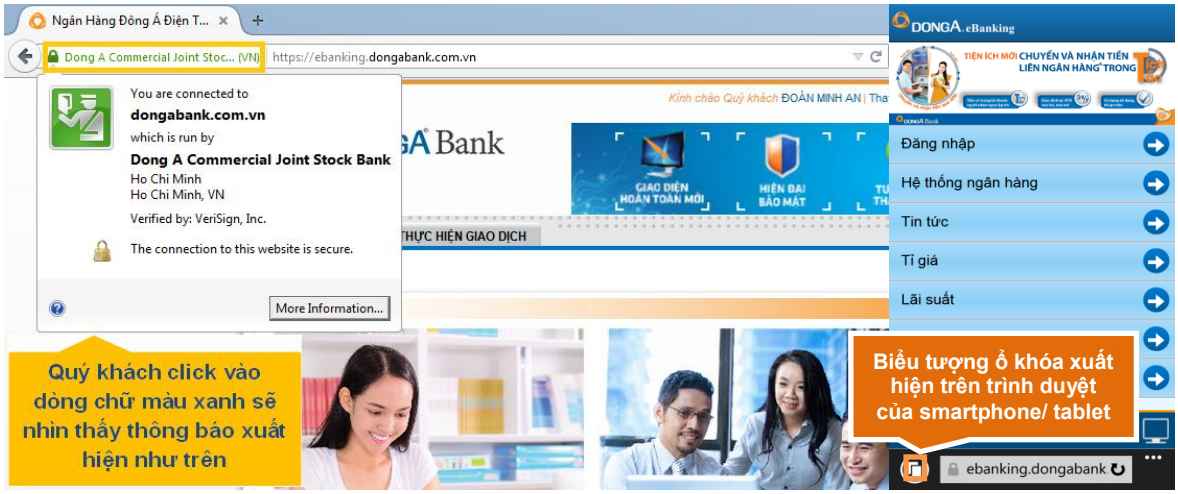
- **Khoá tài khoản thẻ** (cú pháp **DAB KHOA [mật mã SMS Banking]** gửi 8149), hoặc;
- **Gọi điện** đến Tổng đài 1900545464 hoặc đến Chi nhánh/ Phòng giao dịch DongA Bank gần nhất để yêu cầu khóa tài khoản.

- **Đổi mật mã** dịch vụ Ngân hàng Đông Á điện tử trên Internet Banking (mục **Tiện ích/ Đổi mật mã**) hoặc SMS Banking (cú pháp **DAB MM [Mật mã SMS Banking cũ] [Mật mã SMS Banking mới]** gửi 8149).

3. Giải pháp an toàn đối với dịch vụ Ngân hàng Đông Á Điện tử

3.1. Công nghệ mã hoá SSL (Secure Sockets Layer)

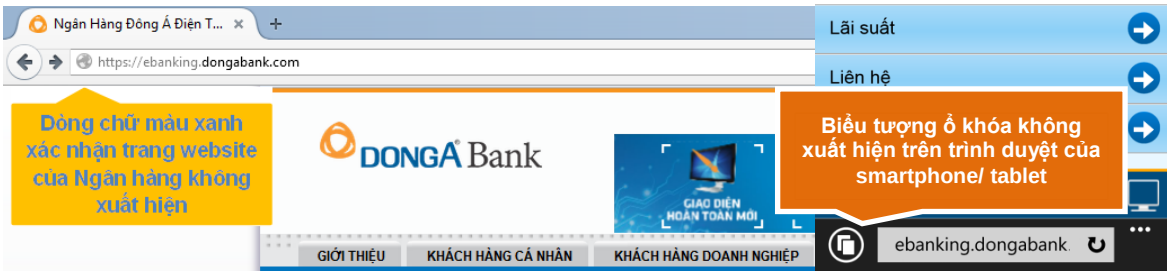
- Một phiên giao dịch an toàn là khi địa chỉ website Internet Banking của DongA Bank tại thanh trình duyệt bắt đầu với **https://** hoặc có biểu tượng ổ khoá xuất hiện tại cửa sổ trình duyệt.
    - **Đối với máy tính:** khi nhấp chuột vào dòng chữ màu xanh trên trình duyệt thì một cửa sổ hiển thị thông 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 chỉ xuất hiện ổ khóa như hình bên dưới.



Hình 7. Hình ảnh ổ khóa chứng nhận an toàn tại thanh địa chỉ

- 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 website này đã được mã hóa để tránh bị nghe trộm thông tin và website này thuộc quyền kiểm soát của DongA Bank.
- Về công nghệ mã hoá SSL được sử dụng tại website của DongA Bank để mã hoá các thông tin cá nhân khi thực hiện kết nối để thực hiện giao dịch, các thông tin được truyền từ thiết bị cá nhân đến DongA Bank 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.
- Đối với những website không an toàn hoặc giả mạo, mặc dù website 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. Bên dưới là ví dụ.



Hình 8. Ví dụ về website giả mạo Internet Banking của DongA Bank

3.2. Ngắt kết nối sau một thời gian ngưng giao dịch

Trường hợp không thực hiện đăng xuất như hướng dẫn tại mục **2.3. Thoát an toàn**, sau khi giao dịch với DongA Bank, sau một thời gian nhất định, hệ thống sẽ tự ngắt phiên đăng nhập để đảm bảo an toàn. Khi muốn thực hiện lại giao dịch mới, khách hàng cần thực hiện đăng nhập từ đầu.

3.3. Yêu cầu đăng nhập đúng Mã số khách hàng/ Tên đăng nhập và mật mã

- Việc truy cập vào Internet Banking/ ứng dụng DongA Mobile Internet Banking chỉ được thành công khi sử dụng đúng Mã số khách hàng/ Tên đăng nhập và mật mã Internet Banking.
- Một giao dịch tài chính chỉ được thực hiện thành công khi nhập đúng mã xác thực OTP được DongA Bank cung cấp thông qua các phương thức xác thực mà khách hàng đã đăng ký với DongA Bank.

3.4. Bắt buộc dùng bàn phím ảo để nhập mật mã

Loại bàn phím ảo này giúp hạn chế người khác theo dõi thao tác khi đăng nhập bằng bàn phím vật lý (trong trường hợp máy tính đang bị bí mật theo dõi bằng chương trình phần mềm theo dõi thao tác bàn phím/ con trỏ chuột - Keylogger).

3.5. Tự động thay đổi mã xác thực OTP

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

- Quá thời gian nhập mã xác thực OTP giao dịch theo quy định.
- Nhập sai mã xác thực OTP 03 (ba) lần cho 01 (một) lần giao dịch.

3.6. Chống đăng nhập tự động

Trong một số tình huống cần thiết, DongA Bank sẽ bật chế độ mã an toàn (captcha) tại màn hình đăng nhập vào Internet Banking, khách hàng cần nhập Mã số khách hàng/ Tên đăng nhập, mật mã và mã an toàn để đăng nhập thành công theo quy định của DongA Bank tại từng thời điểm.