KHUYẾN CÁO AN TOÀN BẢO MẬT

Ngân hàng TMCP Đông Nam Á ("SeABank") cam kết và luôn cố gắng mang đến cho Quý khách hàng dịch vụ Ngân hàng trực tuyến tiện lợi và an toàn nhất. Quý khách hàng và Ngân hàng SeABank đều đóng vai trò quan trọng trong việc bảo vệ các giao dịch tránh khỏi những gian lận trực tuyến. Vì vậy, Ngân hàng SeABank khuyến nghị Quý khách hàng đọc kỹ và tuân thủ các nội dung khuyến cáo sau đây vì an toàn bảo mật thông tin và quyền lợi cá nhân của Quý khách.

1. **Tạo mật khẩu và bảo quản thông tin đăng nhập**

   Quý khách hàng vui lòng thực hiện những khuyến nghị của Ngân hàng SeABank về việc tạo mật khẩu và bảo quản thông tin đăng nhập theo nội dung sau:

   - ✓ Mật khẩu tạo phải có độ dài tối thiểu 8 ký tự, phức tạp, khó đoán.
   - ✓ Tránh tạo mật khẩu dưới dạng tên, số điện thoại, ngày tháng năm sinh hay các thông tin cá nhân khác của Quý khách hàng. Mật khẩu không nên là những từ phổ thông, dễ nhớ, dễ tìm thấy trong từ điển.
   - ✓ Thường xuyên thay đổi mật khẩu (tối thiểu 6 tháng/1 lần), mật khẩu không được lập lại.
   - ✓ Không viết mật khẩu ra giấy hoặc ghi chép mật khẩu dưới hình thức khác.
   - ✓ Tránh dùng chung một mật khẩu cho nhiều dịch vụ khác nhau (ví dụ như Yahoo Mail, Google Mail, v.v.)
   - ✓ Quý khách hàng tự bảo quản thông tin tên đăng nhập, mật khẩu, thiết bị xác thực của mình (điện thoại di động, thiết bị Token), không chia sẻ hay tiết lộ cho người khác biết.
   - ✓ Trong trường hợp có ghi ngờ tên đăng nhập, mật khẩu của mình đã bị lộ hoặc bị người khác sử dụng trái phép, Quý khách cần thông báo ngay với Ngân hàng SeABank để làm các thủ tục ngăn chặn/khóa và thay đổi thông tin.

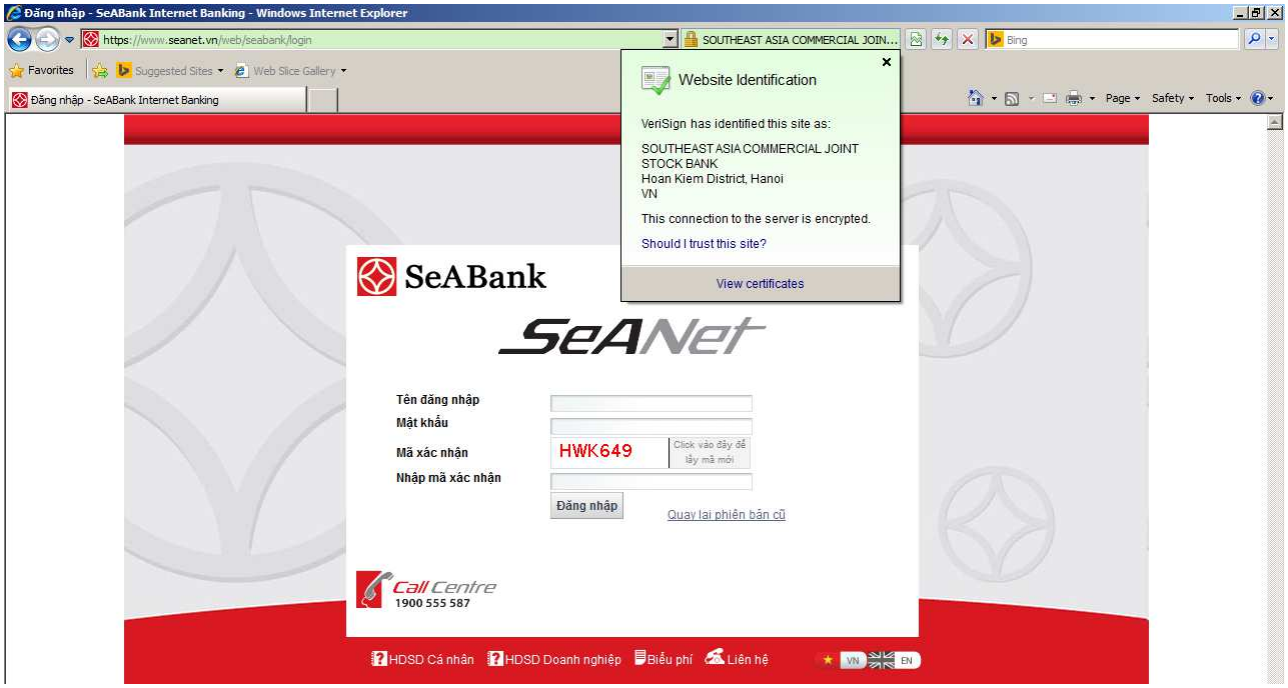
2. **Sử dụng dịch vụ Ngân hàng trực tuyến của SeABank**

   Để đảm bảo an toàn phiên giao dịch trực tuyến và bảo mật các các thông tin giao dịch của Quý khách hàng, khi sử dụng dịch vụ Ngân hàng trực tuyến Internet Banking, Mobile Banking của Ngân hàng SeABank Quý khách vui lòng thực hiện đầy đủ các khuyến cáo sau:

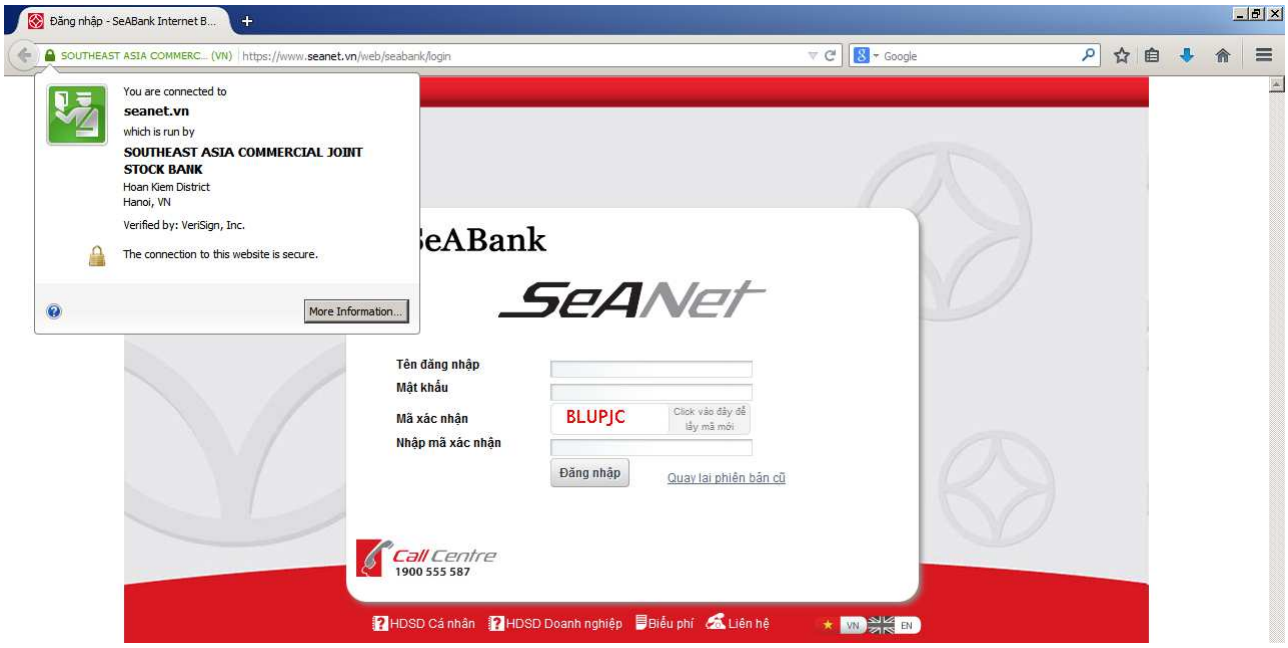
   - ✓ Luôn gõ địa chỉ trang web dịch vụ Ngân hàng trực tuyến của Ngân hàng SeABank https://www.seanet.vn vào thanh địa chỉ của trình duyệt hoặc truy cập thông qua trang mạng chính thức của Ngân hàng SeABank tại địa chỉ http://www.seabank.com.vn. Hai địa chỉ trên là địa chỉ chính thức và duy nhất của Ngân hàng SeABank, Quý khách **KHÔNG ĐƯỢC** đăng nhập thông tin truy cập dịch vụ của mình vào hay thông qua bất kỳ trang mạng nào khác.
   - ✓ Quý khách nên sử dụng các trình duyệt mạng phiên bản mới, có uy tín với tính năng bảo mật tốt như Internet Explorer, Mozilla Firefox, Chrome hay Safari. Trong các

trình duyệt mạng Quý khách không nên kích hoạt tính năng tự động lưu lịch sử và các thông tin truy cập dịch vụ (ví dụ như tên đăng nhập, mật khẩu).

- ✓ Khi truy cập vào trang mạng Ngân hàng trực tuyến của Ngân hàng SeABank, Quý khách lưu ý kiểm tra biểu tượng ổ khóa ( ) chứng nhận và xác thực tính hợp pháp của trang mạng. Một phiên giao dịch trực tuyến an toàn phải có địa chỉ bắt đầu với **https://** và/hoặc có biểu tượng ổ khóa xuất hiện bên cạnh thanh địa chỉ của trình duyệt. Tại trang mạng hợp pháp của dịch vụ Ngân hàng trực tuyến Ngân hàng SeABank khi truy cập sẽ xuất hiện dòng chữ **SOUTHEAST ASIA COMMERCIAL JOINT STOCK BANK** với biểu tượng ổ khóa như trên. Khi Quý khách nhấn vào dòng chữ trên sẽ xuất hiện cửa sổ xác nhận kết nối được mã hóa và chứng nhận trang mạng thuộc quyền quản lý, sở hữu của Ngân hàng TMCP Đông Nam Á **(Southeast Asia Commercial Joint Stock Bank, Hoan Kiem District, Hanoi, VN**)
  - o Hình ảnh trang mạng hợp pháp dịch vụ Ngân hàng trực tuyến của Ngân hàng SeABank trên các trình duyệt:
    - Microsoft Internet Explorer



- Mozilla Firefox



- ✓ Khi không sử dụng dịch vụ hoặc rời khỏi máy, Quý khách hàng nên thoát khỏi phiên giao dịch bằng cách nhấn vào mục **THOÁT** trên màn hình, đóng trình duyệt và khóa máy an toàn.
- ✓ Những kẻ xấu có thể tạo và sử dụng một trang mạng giả mạo giống như trang mạng hợp pháp của Ngân hàng SeABank để đánh lừa và lấy trộm những thông tin giao dịch, nhạy cảm của Quý khách. Vì vậy khi thấy một trang mạng giả mạo ngân hàng SeABank, không đáp ứng đầy đủ những điều kiện trên, Quý khách vui lòng ngừng giao dịch và thông báo ngay với Trung tâm Chăm sóc khách hàng của Ngân hàng SeABank – Call Center: **1800 555 587** (miễn phí, phục vụ 24/7) hoặc hòm thư điện tử email **contact@seabank.com.vn**.

3. Liên lạc với Ngân hàng SeABank

- ✓ Khi gặp các lỗi dịch vụ hay sự cố trong quá trình sử dụng dịch vụ, Quý khách hàng vui lòng liên hệ với Trung tâm Chăm sóc khách hàng của Ngân hàng SeAbank – Call Center: **1800 555 587** để được hỗ trợ, giúp đỡ.
- ✓ Khi Quý khách sử dụng dịch vụ Ngân hàng điện tử của Ngân hàng SeABank với phương thức xác thực qua SMS và bị mất điện thoại hoặc sử dụng loại hình xác thực qua thiết bị Token và bị mất thiết bị Token, Quý khách hàng vui lòng liên hệ với Trung tâm Chăm sóc khách hàng của Ngân hàng SeABank – Call Center: **1800 555 587** hoặc đến điểm giao dịch gần nhất của Ngân hàng SeABank để thông báo và yêu cầu khoá hoặc sửa đổi loại hình xác thực.
- ✓ Trong trường hợp nhận được thư điện tử email hoặc cuộc gọi điện thoại từ người nào tự nhận là từ Ngân hàng SeABank yêu cầu Quý khách cung cấp thông tin cá nhân, thông tin về tài khoản đăng nhập dịch vụ của Quý khách v.v., Quý khách **KHÔNG ĐƯỢC** thực hiện theo yêu cầu đó và thông báo ngay cho Ngân hàng SeABank thông qua **Call Center: 1800 555 587** hoặc hòm thư điện tử email contact@seabank.com.vn. Nguyên tắc bảo mật của Ngân hàng SeABank không bao giờ yêu cầu Quý khách tiết lộ hay cung cấp những thông tin về mật khẩu, mã số PIN hay mật mã ngân hàng của Quý khách thông qua điện thoại hay thư điện tử email.

4. Các khuyến nghị về cài đặt và sử dụng phần mềm, ứng dụng

Trên các thiết bị, máy vi tính dùng để truy cập dịch vụ Ngân hàng trực tuyến của Ngân hàng SeABank Quý khách hàng cần lưu ý những vấn đề sau:

- ✓ Hệ điều hành máy vi tính, thiết bị của Quý khách phải được cập nhật phiên bản mới vá lỗi bảo mật thường xuyên.
- ✓ Cài đặt vả sử dụng phần mềm chống virus/mã độc hại phiên bản mới, cập nhật thông tin cơ sở dữ liệu về virus, mã độc hại mới nhất. Khuyến cáo Quý khách nên sử dụng các phần mềm thương mại có uy tín trong lĩnh vực an toàn, bảo mật như: Kaspersky, Symantec, McAfee…
- ✓ Sử dụng ứng dụng tưởng lửa cá nhân (Personal Firewall) tích hợp sẵn trong hệ điều hành hoặc các phần mềm thương mại có uy tín với khả năng phát hiện xâm nhập như Comodo Internet Security, Kaspersky Internet Security, Zone Alarm…
- ✓ Chỉ sử dụng những phần mềm, ứng dụng hợp pháp, có bản quyền và nguồn gốc rõ ràng. Quý khách hàng không nên cài đặt và sử dụng những phần mềm, ứng dụng, trò chơi, phần mềm chat, nhắn tin miễn phí có nguồn gốc không chính thống, không tin cậy, bị bẻ khóa hoặc chia sẻ trên các diễn đàn, mạng trực tuyến.
- ✓ Không nên mở những tập tin (attachments) lạ, nghi vấn đính kèm thư điện tử email của người quen cũng như người lạ gửi đến, không nhấn vào những đường dẫn liên kết (link, URL) gửi kèm theo thư điện tử email hay tin nhắn khi chưa xác định được mục đích và nguồn gốc.
- ✓ Luôn bảo vệ thiết bị, máy vi tính cá nhân của mình, không cho người lạ mượn hay dùng để kết nối với thiết bị, mạng chưa được kiểm tra. Quý khách cần hạn chế cài đặt các phần mềm, ứng dụng, trò chơi vào thiết bị của mình tại các cửa hàng, địa điểm không tin cậy

Ngân hàng TMCP Đông Nam Á (SeABank)