

KHUYẾN CÁO BẢO MẬT THÔNG TIN

Agribank cam kết và mong muốn mang lại dịch vụ Internet Banking tiện ích và an toàn cho Quý khách hàng. Vì vậy, Agribank khuyến nghị Quý khách hàng một số nội dung khi sử dụng dịch vụ Internet Banking, cụ thể như sau:

1. Về đặt mật khẩu và bảo vệ mật khẩu

Cách đặt mật khẩu

- Mật khẩu đăng nhập có độ dài tối thiểu 06 ký tự, bao gồm các ký tự chữ và số, có chứa chữ hoa và chữ thường hoặc các ký tự đặc biệt. Không được sử dụng toàn bộ ký tự trùng nhau hoặc liên tục theo thứ tự trong bảng chữ cái, chữ số. Thời gian hiệu lực của Mật khẩu đăng nhập tối đa 12 tháng.

- Khách hàng phải thay đổi Mật khẩu đăng nhập ngay lần đăng nhập đầu tiên. Trường hợp khách hàng nhập sai Mật khẩu đăng nhập liên tiếp 05 lần sẽ bị khóa Tên đăng nhập. Khách hàng yêu cầu mở khóa Tên đăng nhập tại quầy giao dịch của chi nhánh nơi khách hàng đăng ký dịch vụ.

- Tránh sử dụng tên, số điện thoại, ngày sinh nhật và các thông tin cá nhân khác của Quý khách hàng để đặt mật khẩu.

Cách bảo vệ mật khẩu

- Quý khách tự bảo quản tên đăng nhập và mật khẩu của mình, không tiết lộ thông tin cho người khác biết.

- Thường xuyên thay đổi mật khẩu.

- Không viết mật khẩu ra giấy hoặc lưu mật khẩu trong điện thoại di động.

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

- Thông báo ngay với Agribank khi Quý khách biết hoặc nghi ngờ mật khẩu của mình bị lộ hoặc user Internet Banking của mình bị người khác sử dụng.

2. Về bảo vệ thiết bị xác thực và mã xác thực

- Không chia sẻ thiết bị OTP Hard Token, Chữ ký số và điện thoại di động với người khác.

- Quý khách tự bảo quản thiết bị xác thực (OTP Hard Token) và/hoặc số điện thoại di động nhận mã xác thực đã đăng ký với Agribank, không để lộ mã xác thực cho người khác biết.

3. Về cách sử dụng trình duyệt web



Quý khách không đặt tùy chọn của trình duyệt web cho phép lưu lại tên và mật khẩu người dùng.

4. Thoát khỏi hệ thống Internet Banking khi không sử dụng

Khi không sử dụng hoặc rời khỏi máy, Quý khách hàng nên thoát khỏi trang giao dịch mà mình đang thực hiện bằng cách lick chuột vào mục ĐĂNG XUẤT trên màn hình và khóa máy.

5. Truy cập đúng website dịch vụ Internet Banking của Agribank

Những kẻ xấu thường 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. Do đó, để đảm bảo an toàn cho các thông tin giao dịch, Agribank khuyến cáo Quý khách:


- Luôn gõ đúng địa chỉ website dịch vụ Internet Banking của Agribank mà Khách hàng muốn giao dịch vào thanh địa chỉ của trình duyệt web:
<https://ibank.agribank.com.vn>

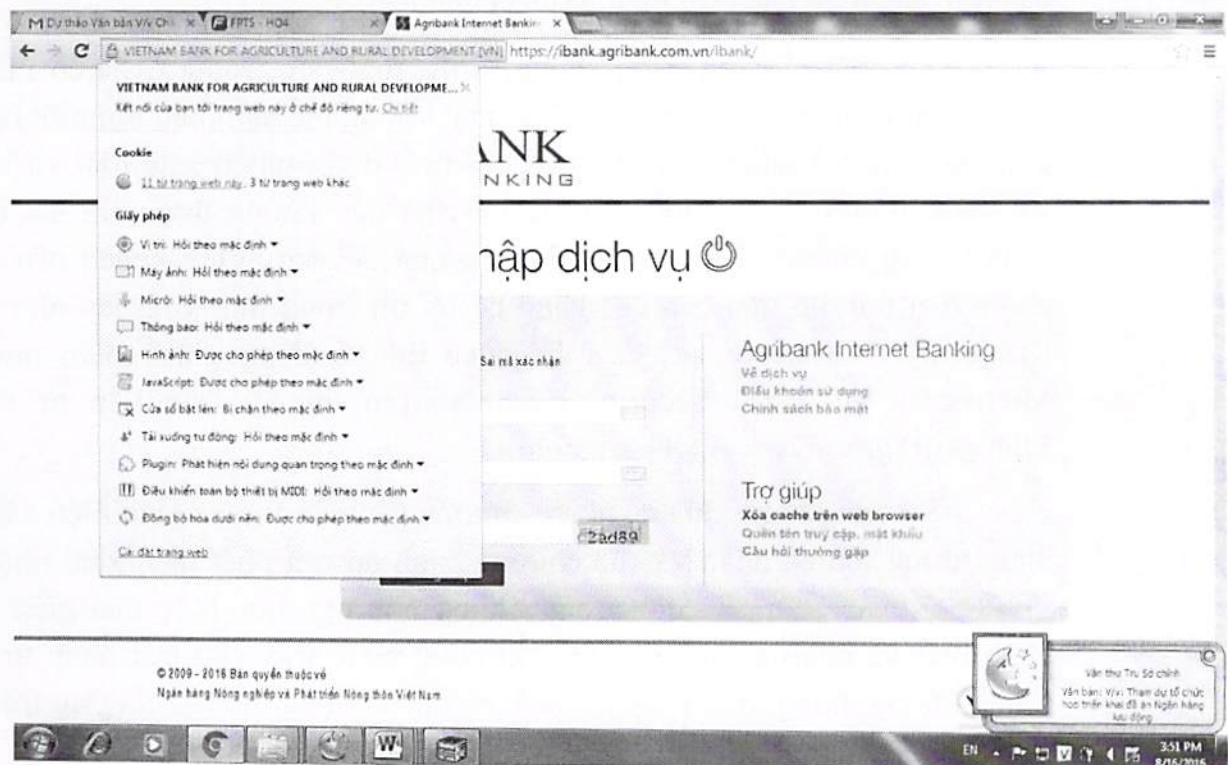
- Quý khách hàng không đăng nhập thông tin tài khoản của mình tại bất kì website nào khác.

- Thận trọng, hạn chế dùng máy tính công cộng, mạng không dây công cộng để truy cập vào hệ thống Internet Banking (Cafe 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: tên truy cập, mật khẩu, mã PIN ...

- Kiểm tra biểu tượng ổ khóa và chứng nhận của website như sau:

+ 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.

+ Tại trang web thật của Agribank, khi Quý khách hàng truy cập, một dòng chữ màu xanh sẽ xuất hiện “VIETNAM BANK FOR AGRICULTURE AND RURAL DEVELOPMENT [VN]” và khi click chuột vào dòng chữ màu xanh nói trên thì một cửa sổ hiển thị thông tin xuất hiện như bên dưới chứng nhận website thuộc quyền kiểm soát của Agribank. 




+ Các website không đảm bảo một trong các điều kiện nêu trên đều có thể là website giả mạo, Quý khách hãy ngừng ngay việc giao dịch và liên hệ với đường dây nóng của Agribank để được hỗ trợ.

6. Thông báo với Agribank khi

- Quý khách gặp các lỗi và sự cố trong quá trình sử dụng dịch vụ.
- Quý khách sử dụng dịch vụ Internet Banking với phương thức xác thực qua OTP SMS Token và bị mất điện thoại hoặc OTP Hard Token.
- Thông báo ngay cho Agribank nếu Quý khách nhận được một thư điện tử khả nghi hoặc một cuộc điện thoại từ một người nào đó 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 Agribank vì Agribank sẽ không bao giờ yêu cầu Quý khách tiết lộ mật khẩu hay Mã xác thực thông qua điện thoại hoặc thư điện tử.

7. Thực hiện theo các khuyến nghị của Agribank về cài đặt phần mềm 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.
- Cài đặt chương trình chống virus, malware, rootkit... 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. Máy tính cá nhân rất dễ bị nhiễm các loại virus, malware, spyware, rootkit từ môi trường internet nếu không được cài đặt các chương trình phòng chống virus một cách hiệu quả. Vì vậy, Quý khách 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"(có thể tải trực tiếp từ website của Microsoft <http://www.microsoft.com>)
- Sử dụng tường lửa cá nhân, chương trình dò tìm và phát hiện xâm nhập: Sử dụng 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 Quý khách nhận biết và ngăn chặn các cuộc tấn công hoặc truy cập trái phép từ những đối tượng không mong muốn. Quý khách có thể sử dụng một số chương trình phổ biến như: Zone Alarm, Patriot ...
- Chỉ nên sử dụng những chương trình hợp pháp. Quý khách không nên 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) và nên sử dụng chương trình quét virus để quét các tập tin trước khi mở chúng. 

**NGÂN HÀNG NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔNG VIỆT NAM**