NGÂN HÀNG NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN VIỆT NAM
AGRIBANK
Mang phồn thịnh đến khách hàng

KHUYẾN CÁO BẢO MẬT THÔNG TIN

Agribank trân trọng cảm ơn Quý Khách hàng đã tin tưởng và sử dụng dịch vụ của chúng tôi. Agribank cam kết và luôn mong muốn cung cấp tới Quý Khách hàng những dịch vụ ngân hàng điện tử tiện ích và an toàn nhất. Vì vậy, Agribank khuyến nghị Quý Khách một số nội dung khi sử dụng các dịch vụ ngân hàng điện tử, cụ thể như sau:

1. VỀ ĐẶT MẬT KHẨU VÀ QUẢN LÝ MẬT KHẨU

1.1. Cách đặt mật khẩu

- Mật khẩu đăng nhập có độ dài tối thiểu 06 ký tự, bao gồm các ký tự chữ, số, có chứa chữ hoa, chữ thường và các ký tự đặc biệt. Thời gian hiệu lực của Mật khẩu đăng nhập tối đa 12 tháng.

- Để đảm bảo an toàn tài sản của Quý Khách, hệ thống Agribank sẽ yêu cầu Quý Khách thay đổi Mật khẩu đăng nhập ngay lần đăng nhập đầu tiên. Trường hợp Quý Khách nhập sai Mật khẩu đăng nhập 05 lần liên tiếp, hệ thống sẽ tự động khóa Tên đăng nhập. Trong trường hợp này, Quý Khách vui lòng đến quầy giao dịch của Agribank để được hỗ trợ mở khóa Tên đăng nhập.

- Để đảm bảo an toàn, bảo mật, Quý Khách tuyệt đối không sử dụng toàn bộ ký tự trùng nhau hoặc liên tục theo thứ tự trong bảng chữ cái, chữ số; Tránh sử dụng tên, số điện thoại, ngày sinh nhật và các thông tin cá nhân dễ nhận biết khác để đặt mật khẩu; Tránh đặt mật khẩu giống nhau cho các website/dịch vụ khác nhau; Không nhờ người khác đặt hộ mật khẩu. Đối với dịch vụ Agribank E-Mobile Banking/phần mềm xác thực Soft OTP dịch vụ Internet Banking: Ngoài mật khẩu thông thường, khách hàng nên sử dụng thêm các hình thức mật khẩu sinh trắc học như khuôn mặt, vân tay…

1.2. Cách quản lý mật khẩu

- Quý Khách tự bảo quản tên đăng nhập và mật khẩu của mình, tuyệt đối không tiết lộ/chia sẻ thông tin liên quan đến tên đăng nhập/mật khẩu/mã PIN, mã xác thực (OTP) với bất kỳ ai.

- Thường xuyên thay đổi mật khẩu, tối thiểu 01 năm 01 lần hoặc khi bị lộ, nghi ngờ bị lộ mật khẩu. Đặc biệt nên thay đổi mật khẩu ngay sau khi truy cập dịch vụ từ thiết bị/mạng công cộng (vui lòng thay đổi mật khẩu tại một thiết bị/đường mạng tin cậy khác).

- Không nên viết mật khẩu ra giấy, lưu trong điện thoại di động hoặc ghi chép dưới bất kỳ hình thức nào; không đọc to mật khẩu để tránh lộ mật khẩu mà

Quý Khách không kiểm soát được.

- Đối với dịch vụ Internet Banking: Không cung cấp/nhập mật khẩu tại bất cứ website ngoài website https://ibank.agribank.com.vn

- Khi sử dụng mật khẩu sinh trắc học vân tay, để đảm bảo an toàn, Quý Khách hàng lưu ý các điều sau:

+ Hệ thống không hỗ trợ đăng nhập bằng vân tay đối với các thiết bị đã jailbreak hoặc rooted. Agribank xin miễn trừ trách nhiệm nếu thiết bị của khách hàng đã jailbreak hoặc rooted.

+ Đảm bảo chỉ sử dụng duy nhất dấu vân tay của khách hàng để mở khóa điện thoại.

+ Không cho mượn điện thoại và không sử dụng đăng nhập bằng vân tay với các điện thoại dùng chung.

+ Trước khi đổi điện thoại, khi sửa chữa hoặc nhờ cài đặt trên thiết bị di động của mình, Quý Khách hàng cần hủy đăng ký chức năng đăng nhập bằng vân tay và đăng xuất khỏi hệ thống.

- Thông báo ngay với Agribank khi Quý Khách biết hoặc nghi ngờ mật khẩu hoặc tên đăng nhập dịch vụ của mình bị người khác sử dụng.

2. BẢO VỆ THIẾT BỊ XÁC THỰC VÀ MÃ XÁC THỰC

- Không chia sẻ thiết bị xác thực và điện thoại di động với người khác.

- Quý Khách tự bảo quản thiết bị xác thực, thiết bị cá nhân cài đặt Soft OTP và/hoặc số điện thoại di động nhận mã xác thực đã đăng ký với Agribank, tuyệt đối không để lộ/cung cấp mã xác thực, mã kích hoạt đăng nhập Soft OTP/Token OTP cho người khác biết.

- Không nhập mã xác thực vào website/màn hình không có dấu hiệu Agribank, không cung cấp mã xác thực để nhận giải thưởng, khuyến mại… Agribank không bao giờ yêu cầu khách hàng cung cấp thông tin mã xác thực để nhận quà/giải thưởng, xác nhận định danh… Trường hợp Quý Khách thường xuyên giao dịch với giá trị cao, Quý Khách có thể lựa chọn hình thức bảo mật nâng cao của Soft OTP, Token OTP; kích hoạt xác thực bằng vân tay nếu điện thoại Quý Khách hỗ trợ tính năng này.

3. THẬN TRỌNG KHI THỰC HIỆN GIAO DỊCH TRỰC TUYẾN

- Xác thực người đề nghị thực hiện giao dịch tài chính: Đối tượng gian lận có thể giả mạo danh tính của người Quý Khách hàng quen biết thông qua mạng xã hội cũng như các kênh liên lạc khác như email, điện thoại, thư giấy, SMS… để lừa đảo, gợi ý khách hàng cho vay/chuyển tiền tới tài khoản của tin tặc.

- Kiểm tra thông tin được sử dụng để thực hiện giao dịch. Chủ động bảo mật thông tin trong các giao dịch online, cẩn trọng với các quảng cáo/ khuyến mại online và không truy cập đường link qua email.

- Agribank đặc biệt khuyến nghị Quý Khách đăng ký dịch vụ thông báo biến động số dư tài khoản thanh toán, tài khoản tiền gửi tiết kiệm, tài khoản vay của mình nhằm kịp thời phát hiện và giảm thiểu rủi ro liên quan đến các giao dịch bất thường.

- Không nạp tiền/chuyển khoản cho người lạ hoặc có dấu hiện nghi vấn. **Cán bộ Agribank và các cơ quan chức năng không bao giờ yêu cầu khách hàng chuyển tiền hay cung cấp thông tin qua email hoặc điện thoại.**

- Khi hoàn thành phiên giao dịch và không có nhu cầu sử dụng hoặc rời khỏi máy, Quý Khách hàng nên thoát khỏi trang giao dịch mà mình đang thực hiện bằng cách ĐĂNG XUẤT/Thoát ứng dụng và khóa máy, không nên thoát khỏi trình duyệt mà không đăng xuất. **TRỌN**

- Khi sử dụng dịch vụ E-Mobile Banking, để Quý Khách nên cài đặt hạn mức giao dịch phù hợp với nhu cầu sử dụng và lưu tên, số tài khoản trong danh bạ đối với các tài khoản thường xuyên giao dịch (khi thực hiện chuyển khoản) để sử dụng cho các lần tiếp theo, tránh chuyển nhầm cho người khác.

4. VỀ SỬ DỤNG DỊCH VỤ INTERNET BANKING CỦA AGRIBANK

4.1. 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.

- Sử dụng các trình duyệt cập nhật mới nhất có chế độ bảo mật tiêu chuẩn hoặc chế độ cao (dịch vụ Internet Banking sử dụng tốt nhất ở trình duyệt Google Chrome).

- Thường xuyên thực hiện xóa history, cache và cookie của trình duyệt Internet. Việc xóa các dữ liệu trên sẽ hạn chế việc thông tin liên quan đến hoạt động truy cập được lưu lại trên máy tính, tạo cơ hội đánh cắp dữ liệu.

4.2. Truy cập đúng website dịch vụ

Để tránh trường hợp kẻ gian sử dụng trang web giả mạo giống như trang web thật của Agribank, lừa Quý Khách hàng nhập các thông tin nhạy cảm của mình và sử dụng thông tin này thực hiện các hành vi trục lợi, gây thiệt hại tài chính hoặc uy tín của Quý Khách hàng, Agribank khuyến cáo Quý khách chủ động bảo vệ thông tin giao dịch của mình bằng cách:

- Luôn gõ đúng địa chỉ website dịch vụ Internet Banking của Agribank vào thanh địa chỉ của trình duyệt web: https://ibank.agribank.com.vn

- Tuyệt đối 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 hệ thống Agribank Internet Banking (Cafe Wifi, trung tâm mua sắm, siêu thị, nhà sách...) vì đây là môi trường thuận lợi cho kẻ gian đánh cắp các thông tin nhạy cảm của Quý Khách như: tên truy cập, mật khẩu, mã PIN…

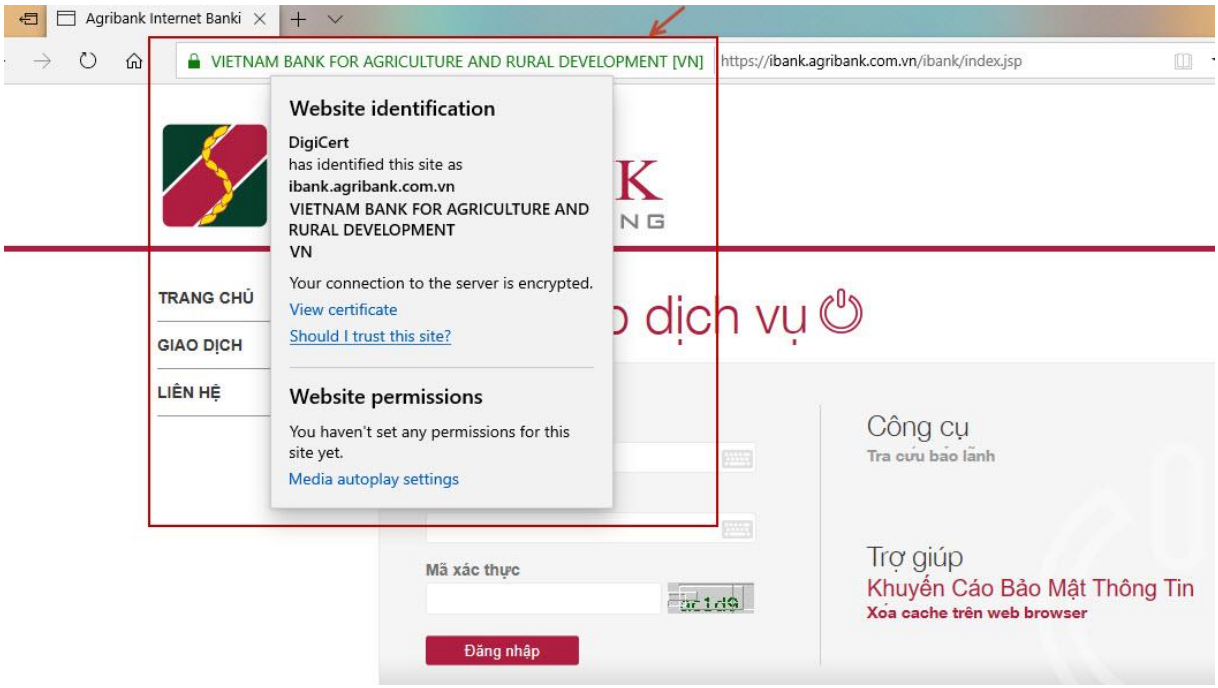
Trường hợp phải dùng máy tính công cộng để đăng nhập dịch vụ, xin hết sức **lưu ý** trong quá trình nhập tên đăng nhập và mật khẩu để bảo vệ tài khoản của mình. Quý Khách nên tìm hiển các cách đăng nhập mật khẩu phòng tránh keylooger, có thể tham khảo một vài cách phòng tránh phần nào quá trình nhận diện mật khẩu như: Nhập vài ký tự trong ô mật khẩu xem kẽ với các ký tự không nằm trong mật khẩu, sau đó dùng phím backspace/delete xóa đi các ký tự thừa; Nhập đoạn sau của mật khẩu trước, sau đó di chuyển lên vị trí đầu để nhập bổ sung phần đầu của mật khẩu; Nhập xen kẽ giữa ô tên đăng nhập và mật khẩu bằng cách di chuyển chuột; Sử dụng bàn phím ảo (virtual keyboard)…

- Kiểm tra tính bảo mật, an toàn của trang web dựa trên các dấu hiệu nhận diện cụ thể:

- URL bắt đầu với https:// và có biểu tượng ổ khoá trên thanh địa chỉ, bên trái địa chỉ web.

+ Thanh địa chỉ trình duyệt chuyển sang màu xanh lá cây có hiển thị tên tiếng Anh đầy đủ của Agribank: “VIETNAM BANK FOR AGRICULTURE AND RURAL DEVELOPMENT [VN]”, trình duyệt web sẽ hiển thị thông tin

chứng nhận website thuộc quyền kiểm soát của Agribank khi Quý Khách kích chọn nội dung này.



+ 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.

4.3. Đảm bảo an toàn khi sử dụng thiết bị di động/ máy tính

- Đảm bảo rằng trên thiết bị di động/ 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… có uy tín (Symantec, Kaspersky, - McAfee, AVG…) trên máy tính cá nhân để phòng chống có hiệu quả các loại virus, malware, spyware, rootkit… xâm nhập từ internet.

- Sử dụng tường lửa cá nhân, chương trình dò tìm và phát hiện xâm nhập máy tính giúp Quý Khách nhận biết và ngăn chặn các cuộc tấn công hoặc truy cập trái phép từ những đối tượng không mong muốn.

- Chỉ nên sử dụng những chương trình hợp pháp, tránh tải và cài đặt vào thiết bị di động/ máy tính cá nhân các chương trình từ những website không hợp pháp hoặc không xác định được nguồn gốc; không mở các tập tin được gửi từ địa chỉ email lạ (không rõ người gửi là ai) và nên sử dụng chương trình quét virus để quét các tập tin trước khi mở.

- Bảo mật kết nối internet của Quý Khách để ngăn chặn các đối tượng can thiệp vào đường mạng, thiết bị của Quý Khách. Cài đặt mật khẩu cho kết nối internet hoặc áp dụng các biện pháp bảo mật theo hướng dẫn của nhà cung cấp.

5. VỀ SỬ DỤNG VÍ ĐIỆN TỬ

Để đảm bảo quyền và lợi ích hợp pháp của Quý Khách, tránh rủi ro khi sử dụng dịch vụ liên kết Ví điện tử, Quý Khách cần lưu ý:

- Không thực hiện các hành vi bị cấm như cho thuê, cho mượn tên và mật khẩu đăng nhập/ tài khoản thanh toán; mua, bán, thuê, cho thuê thẻ hoặc thông tin thẻ, mở hộ thẻ; thuê, cho thuê, mượn, cho mượn Ví điện tử hoặc mua, bán thông tin Ví điện tử...

- Không sử dụng hoặc tạo điều kiện cho các đối tượng sử dụng tên và mật khẩu đăng nhập/ tài khoản thanh toán, thẻ ngân hàng, Ví điện tử vào mục đích vi phạm pháp luật.

6. MỘT SỐ HÌNH THỨC LỪA ĐẢO PHỔ BIẾN

Quý Khách hàng cần nâng cao cảnh giác trong các trường hợp sau:

- Giả mạo thương hiệu, website ngân hàng, ví điện tử với ứng dụng công nghệ cao gửi tin nhắn, email có chứa link lừa đảo yêu cầu Quý Khách hàng truy cập để giao dịch (mua bán online), nhận tiền từ nước ngoài (Western Union), nhận quà tặng, cho vay nhanh…

- Giả mạo cán bộ ngân hàng, tổng đài chăm sóc khách hàng gọi điện yêu cầu khách hàng cung cấp các thông tin cá nhân, tài khoản, thẻ… để nhận tiền, quà trúng thưởng…

- Giả mạo là người cho vay trực tuyến để lừa khách có nhu cầu vay vốn và yêu cầu cung cấp thông tin về thẻ hoặc tài khoản ngân hàng điện tử.

- Giả mạo cơ quan chức năng (tòa án, công an…) gọi điện đe dọa khách hàng có liên quan đến vụ án, đường dây tội phạm và yêu cầu chuyển tiền đến tài khoản gian lận để chạy án.

- Giả mạo người thân, bạn bè nhờ mua thẻ điện thoại, mượn tiền, thanh toán chuyển khoản đến tài khoản gian lận do bị hack Facebook, Messenger, Zalo…

- Giả mạo tài khoản, làm quen nhờ mở tài khoản/đăng ký dịch vụ ngân hàng điện tử hoặc mua lại với giá cao để sử dụng vào mục đích lừa đảo.

7. LIÊN HỆ, THÔNG BÁO VỚI AGRIBANK

Quý khách liên lạc Tổng đài Chăm sóc khách hàng Agribank 1900558818 hoặc điểm giao dịch gần nhất của Agribank trong các trường hợp sau:

- Quý Khách gặp các lỗi và sự cố trong quá trình sử dụng dịch vụ.

- Quý Khách bị mất điện thoại hoặc có bất kỳ sự thay đổi nào về số điện thoại đã đăng ký với Agribank.

- Quý Khách sử dụng dịch vụ Internet Banking với phương thức xác thực qua OTP SMS Token và bị mất điện thoại hoặc mất Token OTP/thiết bị cài đặt Soft OTP. Token OTP bị hư hỏng, gặp sự cố.

- Quý Khách được một thư điện tử khả nghi hoặc một cuộc điện thoại từ một người nào đó yêu cầu Khách hàng nhập các thông tin đăng nhập của mình. Khách hàng tuyệt đối KHÔNG 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 Khách hàng tiết lộ mật khẩu hay Mã xác thực thông qua điện thoại hoặc thư điện tử**.

- Quý Khách nhận được thông báo trúng thưởng hoặc nhận tiền từ nước ngoài chuyển về qua mạng xã hội (Facebook, Zalo…) và yêu cầu cung cấp thông tin, mã xác thực, liên kết ví…

- Quý Khách phát hiện bị lộ thông tin tài khoản hoặc bị lừa đảo hoặc nghi ngờ bị lừa đảo, bị tin tặc hoặc nghi ngờ bị tin tặc tấn công.

Ngoài ra, nếu phát hiện có yêu cầu người lạ thông báo là cán bộ cơ quan điều tra, cán bộ ngân hàng… yêu cầu chuyển tiền, hoặc nghi ngờ/phát hiện bị lừa đảo… Quý Khách vui lòng liên hệ ngay với cơ quan chức năng để trình báo.

NGÂN HÀNG NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔNG VIỆT NAM