VIETBANK

THÔNG BÁO

CẢNH BÁO NGUY CƠ LỪA ĐẢO QUA KÊNH GD NGÂN HÀNG ĐIỆN TỬ

Kính gửi: ***Quý Khách hàng***

Thời gian gần đây, tại Việt Nam xuất hiện một số trường hợp lừa đảo, chiếm đoạt tài sản qua kênh giao dịch Ngân hàng điện tử. Đối tượng phạm tội thường sử dụng điện thoại, email, mạng xã hội hay các website giả mạo; ứng dụng (app) độc hại để khai thác thông tin (tên truy cập, mật khẩu đăng nhập Internet Banking, Mobile Banking, mã xác thực - OTP, số thẻ tín dụng….) và thực hiện chuyển khoản/rút tiền từ chính tài khoản của Khách hàng.

Một số cách thức bọn phạm tội thường sử dụng:

1. Làm quen và đề nghị Khách hàng mở tài khoản, đăng ký dịch vụ Ngân hàng điện tử, sau đó mua lại với giá cao, nhằm sử dụng vào mục đích lừa đảo, rút tiền mặt tại nước ngoài hoặc chuyển tiền.
2. Hướng dẫn Khách hàng đăng nhập vào các website giả mạo hoặc đề nghị Khách hàng tải các ứng dụng độc hại, từ đó đánh cắp tên truy cập, mật khẩu đăng nhập, mã OTP.
3. Giả danh là cán bộ công an, Viện kiểm sát hoặc an ninh ngân hàng gọi điện thông báo tài khoản của Khách hàng bị tội phạm xâm nhập và yêu cầu cung cấp số tài khoản, mật khẩu.
4. Giả danh là nhân viên ngân hàng gọi điện hỏi thăm để tìm cách khai thác thông tin; hoặc thông báo Khách hàng đã trúng thưởng, yêu cầu hoàn tất thủ tục nhận thưởng bằng cách nạp tiền vào số điện thoại chỉ định/chuyển tiền vào tài khoản của bọn tội phạm.

Nhằm chủ động ngăn ngừa các hành vi lừa đảo nêu trên, VietBank khuyến nghị Quý Khách hàng lưu ý thực hiện một số biện pháp sau:

- **KHÔNG** đứng tên hộ người khác để mở tài khoản, mở thẻ và đăng ký dịch vụ Ngân hàng điện tử.
- Luôn đăng nhập đúng địa chỉ VietBank Internet Banking là https://online.vietbank.com.vn, đồng thời, cập nhật thường xuyên Hướng dẫn đảm bảo an toàn trong giao dịch Ngân hàng điện tử và các cảnh báo của Vietbank trên địa chỉ website này.
- Cài đặt đúng ứng dụng "**VietBank M-Plus**" trên Google Plays (với thiết bị Android), hoặc Apple App Store (đối với hệ điều hành iOS) và Windows Phone Store (đối với thiết bị Windows Phone). **KHÔNG** cài đặt các ứng dụng không rõ nguồn gốc hoặc từ các link rác trên Facebook, Email, SMS…
- **KHÔNG** nhập thông tin tên truy cập, mật khẩu đăng nhập Internet Banking/Mobile Banking, mã OTP, số tài khoản… của mình vào một liên kết khác với trình duyệt web của Vietbank hoặc ứng dụng khác với VietBank M-Plus.
- Khi nhận được các cuộc gọi lạ, có dấu hiệu nghi vấn, Khách hàng bình tĩnh, tìm hiểu và xác thực thông tin. Đặc biệt là **KHÔNG** nạp tiền/chuyển tiền theo yêu cầu của người lạ.
- Cảnh giác trước những thủ đoạn khai thác thông tin cá nhân, tài khoản và thông tin thẻ. Tuyệt đối **KHÔNG** cung cấp tên truy cập, mật khẩu đăng nhập Internet Banking, Mobile Banking, mã OTP cho người khác. Quản lý và giữ bí mật số thẻ, ngày hết hạn, số CVV2 ở mặt sau của thẻ tín dụng.
- Chú ý theo dõi SMS/Email thông báo giao dịch để kịp thời nhận thấy các dấu hiệu bất thường.
- Khi có bất kỳ nghi vấn liên quan đến việc lừa đảo thông qua giao dịch tại VietBank, Khách hàng cần báo ngay cho cơ quan chức năng, đồng thời thông báo cho VietBank theo số điện thoại **1800 1122** hoặc bất kỳ điểm giao dịch của VietBank trên toàn quốc, để cùng phối hợp giải quyết.

VietBank kính thông báo đến Quý Khách hàng biết và cảnh giác.

Trân trọng./.