



**Những Hành Vi Bị Cấm
Về Mở Và Sử Dụng Tài Khoản Thanh Toán;
Cảnh Báo Các Hình Thức Lừa Đảo Chiếm Đoạt Tài Sản
Trên Không Gian Mạng;
Những Hành Vi Bị Cấm Khi Phát Hành Và Sử Dụng
Thẻ Ghi Nợ Nội Địa Trên Ứng Dụng TNEX**

Kính gửi: Quý Khách hàng

Trước tiên, Ngân hàng TMCP Hàng Hải Việt Nam (“MSB”) xin chân thành cảm ơn Quý Khách hàng/Đối tác đã quan tâm/sử dụng các sản phẩm dịch vụ ngân hàng của chúng tôi.

MSB xin thông báo đến Quý Khách **“Những hành vi bị cấm về mở và sử dụng tài khoản thanh toán tại MSB”; “Những cảnh báo về các hình thức lừa đảo chiếm đoạt tài sản trên không gian mạng” và “Những hành vi bị cấm khi phát hành và sử dụng thẻ ghi nợ nội địa trên ứng dụng TNEX”** như sau:

**I. NHỮNG HÀNH VI BỊ CẤM VỀ MỞ VÀ SỬ DỤNG
TÀI KHOẢN THANH TOÁN**

- 1) Sửa chữa, tẩy xóa phương tiện thanh toán, chứng từ thanh toán không đúng quy định pháp luật; làm giả phương tiện thanh toán, chứng từ thanh toán; lưu giữ, lưu hành, chuyển nhượng, sử dụng phương tiện thanh toán giả.

- 2) Xâm nhập hoặc tìm cách xâm nhập, đánh cắp dữ liệu, phá hoại, làm thay đổi trái phép chương trình phần mềm, dữ liệu điện tử sử dụng trong thanh toán; lợi dụng lỗi hệ thống mạng máy tính để trục lợi.
- 3) Cung cấp không trung thực thông tin có liên quan đến việc cung ứng hoặc sử dụng dịch vụ thanh toán, dịch vụ trung gian thanh toán.
- 4) Tiết lộ, cung cấp thông tin về số dư trên tài khoản thanh toán, số dư thẻ ngân hàng, số dư ví điện tử và các giao dịch thanh toán của khách hàng tại tổ chức cung ứng dịch vụ thanh toán, tổ chức cung ứng dịch vụ trung gian thanh toán không đúng theo quy định của pháp luật có liên quan.
- 5) Mở hoặc duy trì tài khoản thanh toán, ví điện tử nặc danh, mạo danh; mua, bán, thuê, cho thuê, mượn, cho mượn tài khoản thanh toán, ví điện tử; thuê, cho thuê, mua, bán, mở hộ thẻ ngân hàng (trừ trường hợp thẻ trả trước vô danh); lấy cắp, thông đồng để lấy cắp, mua, bán thông tin tài khoản thanh toán, thông tin thẻ ngân hàng, thông tin ví điện tử.
- 6) Thực hiện, tổ chức thực hiện hoặc tạo điều kiện thực hiện các hành vi: sử dụng, lợi dụng tài khoản thanh toán, phương tiện thanh toán, dịch vụ thanh toán, dịch vụ trung gian thanh toán để đánh bạc, tổ chức đánh bạc, gian lận, lừa đảo, kinh doanh trái pháp luật và thực hiện các hành vi vi phạm pháp luật khác.
- 7) Sử dụng tài khoản thanh toán để thực hiện các giao dịch cho mục đích rửa tiền, tài trợ khủng bố và phổ biến vũ khí hủy diệt hàng loạt, vi phạm chính sách cấm vận trừng phạt.

- 8) Nguồn tiền sử dụng qua tài khoản thanh toán có nguồn gốc bất hợp pháp, liên quan đến các hành vi rửa tiền, tài trợ khủng bố và phổ biến vũ khí hủy diệt hàng loạt, vi phạm chính sách cấm vận trừng phạt.
- 9) Chủ tài khoản thanh toán có tài khoản thanh toán tại tổ chức cung ứng dịch vụ thanh toán nhưng cung cấp thông tin hoặc cam kết không có tài khoản thanh toán tại tổ chức cung ứng dịch vụ thanh toán cho các bên có quyền, nghĩa vụ liên quan theo quy định của pháp luật về giải ngân vốn cho vay của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài.
- 10) Ủy thác, giao đại lý cho tổ chức, cá nhân khác thực hiện hoạt động được phép theo Giấy phép hoạt động cung ứng dịch vụ trung gian thanh toán.
- 11) Hoạt động không đúng nội dung quy định trong Giấy phép hoạt động cung ứng dịch vụ trung gian thanh toán.

II. CẢNH BÁO CÁC HÌNH THỨC LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN TRÊN KHÔNG GIAN MẠNG

Hiện nay với sự phát triển của khoa học, kỹ thuật và công nghệ thông tin, quá trình chuyển đổi số đang diễn ra toàn diện mang lại nhiều tiện ích cho Khách hàng nhưng đồng thời cũng là cơ hội để tội phạm công nghệ cao lợi dụng, thực hiện các hành vi lừa đảo, chiếm đoạt tài sản. Để chủ động phòng ngừa, bảo vệ an toàn tài sản của Khách hàng. MSB mong muốn những thông tin hữu ích về các thủ đoạn lừa đảo dưới đây có thể bảo vệ tất cả khách



hàng, để không ai bị sập bẫy bởi bất kỳ chiêu thức gian lận nào của kẻ gian.

1) Lừa tải ứng dụng giả mạo Dịch vụ công, có chứa mã độc đánh cắp thông tin tài khoản

Đối tượng tự xưng là cán bộ công an phường, thuế, kho bạc,... đề nghị người dân tải và cài đặt ứng dụng giả mạo Dịch vụ công, Thuế, VneID, ...thông qua các tệp có đuôi *.apk hoặc từ kho ứng dụng trên điện thoại hệ điều hành Android. Các ứng dụng này đều có mã độc, yêu cầu cấp toàn bộ quyền truy cập/kiểm soát điện thoại để ghi lại mọi thao tác trên điện thoại của khách hàng, từ đó chiếm đoạt tiền từ tài khoản khách hàng qua ứng dụng ngân hàng điện tử.

2) Giả danh nhân viên ngân hàng nâng hạn mức, mở thẻ tín dụng

Đối tượng giả mạo nhân viên ngân hàng tiếp cận chủ thẻ để tư vấn nâng hạn mức thẻ tín dụng. Đối tượng sẽ hướng dẫn truy cập đường link giả mạo có giao diện tương tự website của MSB sau đó yêu cầu chủ thẻ nhập thông tin thẻ và mã OTP lên website đó. Nếu chủ thẻ thực hiện theo thì sẽ bị mất thông tin thẻ và phát sinh giao dịch trừ tiền trên thẻ.

3) Giả mạo người thân nhờ chuyển tiền, vay tiền qua mạng xã hội

Đối tượng lừa đảo sử dụng tài khoản mạng xã hội đã chiếm được hoặc tạo tài khoản giả có ảnh của khách hàng, để nhắn tin/chat cho người thân trong danh sách bạn bè để hỏi vay tiền hoặc nhờ chuyển tiền vào tài khoản ngân hàng có họ tên trùng

với chủ tài khoản mạng xã hội. Đối tượng còn có thể thực hiện cuộc gọi video giả mạo bằng công nghệ Deepfake nhằm tăng độ tin cậy để nạn nhân chuyển tiền cho đối tượng lừa đảo.

4) Giả mạo tin nhắn mạo danh ngân hàng SMS Brandname

Các tin nhắn giả mạo được lưu trong cùng mục với tin nhắn thật của ngân hàng trên điện thoại có chứa đường link dẫn đến website giả mạo của ngân hàng yêu cầu khách hàng nhập thông tin cá nhân và thông tin tài khoản ngân hàng. Nếu thực hiện theo, kẻ gian sẽ có được mật khẩu và OTP để chiếm đoạt tiền từ tài khoản của khách hàng.

5) Lừa đảo tuyển cộng tác viên online làm nhiệm vụ trên sàn thương mại điện tử nhận quà/tiền hoa hồng

Đối tượng giả mạo yêu cầu nạn nhân đặt mua các đơn hàng ảo nhưng chuyển khoản thanh toán thật, sau đó sẽ được nhận lại tiền gốc cộng hoa hồng. Ban đầu các đơn hàng thường trị giá nhỏ được chuyển trả đầy đủ tiền gốc và hoa hồng để lấy lòng tin. Tiếp đó, đối tượng sẽ yêu cầu thực hiện các nhiệm vụ có giá trị lớn lên và có các lý do để không chuyển lại tiền. Đối tượng yêu cầu CTV tiếp tục thực hiện nhiệm vụ đến khi nạn nhân không còn khả năng chuyển tiền nữa thì lúc đấy nạn nhân mới nhận ra mình đã bị lừa đảo.

Nhằm phòng tránh các nguy cơ bị mất tiền, khách hàng lưu ý một số khuyến cáo bảo mật thông tin cá nhân và tài khoản ngân hàng như sau:

- 1) Tắt quyền trợ năng Accessibility trên thiết bị Android với tất cả các ứng dụng đang sử dụng quyền này.**



- 2) **Không cung cấp** thông tin cá nhân, giấy tờ tùy thân cho bất kỳ ai qua các ứng dụng mạng xã hội (kể cả nhân viên ngân hàng).
- 3) **Không cung cấp** thông tin thẻ/tài khoản, thông tin đăng nhập dịch vụ ngân hàng điện tử, mã OTP cho bất kỳ ai (kể cả nhân viên ngân hàng) và trên các đường link lạ. **MSB không bao giờ yêu cầu khách hàng cung cấp OTP hay bất kỳ mật khẩu nào.**
- 4) **Luôn luôn xác thực** danh tính người nhận trước khi chuyển tiền bằng cách gọi điện trực tiếp vào số điện thoại của người nhận. Không gọi xác thực qua ứng dụng chat (bao gồm cả video call)
- 5) Ưu tiên sử dụng các tính năng bảo mật sinh trắc học như nhận dạng vân tay hoặc khuôn mặt cho các ứng dụng giao dịch tài chính.
- 6) **Nếu phát hiện có dấu hiệu lừa đảo, khách hàng cần liên hệ ngay với cơ quan Công an** để kịp thời giải quyết theo quy định.
- 7) **Chia sẻ** thông tin này với người thân, bạn bè để cùng nâng cao cảnh giác.

Nếu phát hiện dấu hiệu lừa đảo, Quý khách vui lòng liên hệ đến MSB qua các kênh chính thức dưới đây để được hỗ trợ lập tức:

- Hotline: 1800 599 982 (Miễn phí)

Thông tin về “**Những hành vi bị cấm về mở và sử dụng tài khoản thanh toán tại MSB**” và “**Những cảnh báo về các**



hình thức lừa đảo chiếm đoạt tài sản trên không gian mạng” tạo thành một thỏa thuận hoàn chỉnh, không tách rời với Thỏa thuận mở và sử dụng tài khoản thanh toán.

III. NHỮNG HÀNH VI BỊ CẤM KHI PHÁT HÀNH VÀ SỬ DỤNG THẺ GHI NỢ NỘI ĐỊA TRÊN ỨNG DỤNG TNEX

- 1) Sửa chữa, tẩy xóa thẻ, chứng từ thanh toán không đúng quy định pháp luật; làm giả thẻ, chứng từ thanh toán; lưu giữ, lưu hành, chuyển nhượng, sử dụng thẻ giả
- 2) Thuê, cho thuê, mua, bán, mở hộ thẻ; lấy cắp, thông đồng để lấy cắp, mua, bán thông tin thẻ ngân hàng.
- 3) Sử dụng thẻ không hợp pháp.
- 4) Thực hiện, tổ chức thực hiện hoặc tạo điều kiện thực hiện các hành vi: sử dụng, lợi dụng thẻ để đánh bạc, tổ chức đánh bạc, gian lận, lừa đảo, kinh doanh trái pháp luật và thực hiện các hành vi vi phạm pháp luật khác.
- 5) Thực hiện, tổ chức thực hiện hoặc tạo điều kiện thực hiện các hành vi: sử dụng, lợi dụng thẻ để thực hiện các giao dịch gian lận, giả mạo; giao dịch thanh toán không tại Đơn vị chấp nhận thanh toán (ĐVCNT).
- 6) Lấy cắp, thông đồng để lấy cắp thông tin thẻ; tiết lộ và cung cấp thông tin thẻ (bao gồm cả thông tin thẻ hiển thị trên ứng dụng MSB mBank) và thông tin cá nhân của Chủ thẻ; tiết lộ và cung cấp mã PIN, OTP và các yếu tố xác thực khác (mật

khẩu, OTP Token, mã xác thực trên Ứng dụng TNEX,) và giao dịch thẻ không đúng quy định của pháp luật.

- 7) Xâm nhập hoặc tìm cách xâm nhập, đánh cắp dữ liệu, phá hoại, làm thay đổi trái phép chương trình phần mềm, dữ liệu điện tử sử dụng trong thanh toán; lợi dụng lỗi hệ thống mạng máy tính để trục lợi.
- 8) Xâm nhập hoặc tìm cách xâm nhập trái phép, phá hủy chương trình hoặc cơ sở dữ liệu của hệ thống phát hành, thanh toán thẻ, chuyển mạch thẻ, bù trừ điện tử giao dịch thẻ.
- 9) Sử dụng hoặc tạo điều kiện cho các đối tượng sử dụng thẻ để thực hiện các giao dịch vi phạm các quy định cấm vận của MSB hoặc cho các mục đích lừa đảo gian lận, rửa tiền, tài trợ khủng bố, tài trợ phổ biến vũ khí hủy diệt hàng loạt, các giao dịch mua bán tiền ảo, cá độ, đánh bạc trực tuyến, các giao dịch chuyển tiền/nạp tiền vào tài khoản/ví điện tử tại nước ngoài, kinh doanh trái pháp luật... và thực hiện các hành vi vi phạm pháp luật khác.
- 10) Các hành vi bị cấm khác theo quy định của pháp luật.
Ngoài ra, Chủ thẻ cần đảm bảo An toàn trong sử dụng thẻ, bảo quản thẻ và bảo mật các thông tin quan trọng liên quan đến thẻ, không chuyển nhượng thẻ hay đưa thẻ cho người khác sử dụng, không tiết lộ thông tin bảo mật cho bất kỳ ai.
- 11) Khi phát hiện có bất thường (phát sinh các giao dịch bằng thẻ nhưng Chủ thẻ không thực hiện hoặc khi thẻ bị mất cắp, thất lạc, lộ thông tin,...), cần chủ động khóa thẻ trên kênh ngân



hàng điện tử, thông báo và thực hiện các bước theo quy định của MSB.

- 12) Thông tin về “Những hành vi bị cấm khi phát hành và sử dụng thẻ ghi nợ nội địa trên Ứng dụng TNEX” tạo thành một thỏa thuận hoàn chỉnh, không tách rời với Thỏa thuận đăng ký và phát hành thẻ ghi nợ nội địa.

Quý Khách hàng nghiên cứu, xem xét kỹ lưỡng các nội dung nêu trên trước khi quyết định tích chọn Tôi đã đọc & Đồng ý như là bằng chứng về sự Đồng Ý của Quý Khách hàng trong quá trình sử dụng Tài khoản thanh toán tại MSB và sử dụng Thẻ ghi nợ nội địa tại MSB.

Chân thành cảm ơn sự hợp tác của Quý Khách Hàng!