

BIỆN PHÁP ĐẢM BẢO AN TOÀN, BẢO MẬT SỬ DỤNG ỨNG DỤNG TNEX

1. Bảo vệ thông tin đăng nhập và thiết bị

- Khách hàng có trách nhiệm bảo vệ thiết bị nhận mã xác thực giao dịch, mã SMS OTP, tên đăng nhập, mã khóa bí mật của mình để ngăn chặn việc người khác thực hiện giao dịch trái phép. Ứng dụng TNEX không chịu trách nhiệm đối với những thiệt hại về tài chính và phi tài chính trong trường hợp Khách hàng để người khác sử dụng các thông tin trên.
- Không lưu lại tên đăng nhập và mã khóa bí mật, mã xác thực giao dịch trên các trình duyệt.
- Thoát khỏi phần mềm ứng dụng TNEX khi không sử dụng.

2. Thiết lập và thay đổi mật khẩu

- Nguyên tắc thiết lập mã khóa bí mật: độ dài tối thiểu 08 ký tự, bao gồm tối thiểu các thành phần sau: chữ cái viết hoa, chữ cái viết thường, chữ số và ký tự đặc biệt (@#\$\$%^+=).

3. Môi trường sử dụng và thiết bị an toàn

- Khách hàng không nên sử dụng máy tính công cộng để truy cập, thực hiện giao dịch; không nên sử dụng mạng WIFI công cộng khi sử dụng dịch vụ Ứng dụng TNEX.
- Không sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng TNEX, thiết bị nhận mã xác thực giao dịch.
- Không cài đặt các phần mềm lạ, phần mềm không có bản quyền, phần mềm không rõ nguồn gốc.

4. Cập nhật và bảo vệ phần mềm

Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành, phần mềm ứng dụng TNEX; xem xét cài đặt phần mềm phòng chống mã độc và cập nhật mẫu nhận diện mã độc mới nhất trên thiết bị cá nhân sử dụng để giao dịch.

5. Hình thức xác nhận giao dịch

Dịch vụ trên Ứng dụng TNEX hiện cung cấp và áp dụng các hình thức xác nhận giao dịch bao gồm:

- Tên đăng nhập, mã khóa bí mật;
- OTP: SMS OTP, Soft OTP loại nâng cao;
- Hình thức xác nhận khớp đúng thông tin sinh trắc học thiết bị;
- Hình thức xác nhận khớp đúng thông tin sinh trắc học.

Khách hàng sử dụng các hình thức xác nhận giao dịch phù hợp với quy định pháp luật khi thực hiện các giao dịch tài chính trên Ứng dụng TNEX theo yêu cầu của MSB và/hoặc đăng ký của Khách hàng.

6. Nhận diện và phòng tránh rủi ro lừa đảo

- Khách hàng chủ động nhận biết các tình huống lừa đảo, giả mạo trang thông tin điện tử hoặc phần mềm ứng dụng TNEX, và thông báo ngay đến Tổng đài Chăm sóc Khách hàng TNEX qua số 1800.599.982.
- Khách hàng đọc kỹ mục Cảnh báo các hình thức lừa đảo chiếm đoạt tài sản trên không gian mạng tại <https://consumer-images.tnex.com.vn/pdf/nhung-hanh-vi-bi-cam-ve-mo-va-su-dung-tai-khoan-thanh-toan-va-the-ghi-no-noi-dia.pdf> nhằm nắm bắt rủi ro liên quan đến việc sử dụng dịch vụ ngân hàng.

7. Xử lý khi có sự cố hoặc dấu hiệu bất thường

Trường hợp như phát hiện giao dịch bất thường, mất hoặc thất lạc số điện thoại nhận SMS, nghi ngờ bị lừa đảo hoặc bị tin tặc tấn công, khách hàng vui lòng liên hệ ngay với Tổng đài TNEX qua số 1800.599.982 để được hướng dẫn cách xử lý và hỗ trợ kịp thời.