

HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN NGÂN HÀNG ĐIỆN TỬ

1. Bảo mật thông tin tài khoản

- Khách hàng tuyệt đối không cung cấp bất kỳ thông tin bảo mật dịch vụ như: Mã truy cập, mật khẩu truy cập, mã xác thực giao dịch OTP (Soft OTP/hoặc sinh ra trên thiết bị Smart OTP) cho bất kỳ ai và qua bất kỳ hình thức nào như: điện thoại, email, mạng xã hội, ứng dụng, website, đường link lạ, ...;
- NCB không bao giờ yêu cầu Quý khách cung cấp thông tin bảo mật tài khoản;
- Khách hàng tuyệt đối không được mua/bán/thuê/cho thuê/đưa tài khoản cho người khác sử dụng hoặc thực hiện bất kỳ hành vi bất hợp pháp khác;
- Khách hàng thường xuyên cập nhật hướng dẫn giao dịch an toàn để đảm bảo sử dụng các dịch vụ Ngân hàng điện tử đúng cách, an toàn, bảo mật;
- Khách hàng cần thông báo ngay cho NCB qua hotline số 028.38216216/ 18006166 hoặc CN/PGD gần nhất hoặc chủ động khóa dịch vụ qua Internet Banking/ ứng dụng NCB IziMobiz khi:
 - + Bị mất hoặc lộ thông tin tài khoản (tên đăng nhập, mật khẩu, OTP, mã kích hoạt, ...)
 - + Mất/thất lạc thiết bị di động, thiết bị Smart OTP,
 - + Phát hiện các đường link, website, ứng dụng giả mạo hoặc các hành động hỏi về tên đăng nhập, mật khẩu, thông tin cá nhân, ...

2. Lưu ý tên đăng nhập và mật khẩu

- Khách hàng phải đăng ký người dùng có vai trò nhập lệnh và người dùng có vai trò duyệt lệnh là 2 người khác nhau. Hai người dùng này phải có các thông tin, số điện thoại riêng biệt. Người dùng có vai trò duyệt lệnh phải là Người đại diện hợp pháp đăng ký trên hồ sơ mở tài khoản và dịch vụ với NCB;
- Tên đăng nhập phải có tối thiểu 06 (sáu) ký tự liền nhau, được phép bao gồm: chữ cái thường, chữ in hoa không dấu và số; không sử dụng toàn bộ các ký tự trùng nhau hoặc liên tục theo thứ tự trong bảng chữ cái, chữ số;
- Mật khẩu phải có tối thiểu 08 (tám) ký tự liền nhau, bao gồm bắt buộc ít nhất 01 (một) ký tự chữ viết hoa, 01 (một) ký tự chữ viết thường, 01 (một) ký tự số và 01 (một) ký tự đặc biệt. Không đặt mật khẩu dễ đoán như: Mã số thuế, ngày sinh, số điện thoại hoặc các dãy số, chữ cái liên tục hoặc trùng tên đăng nhập... Mật khẩu có hiệu lực tối đa 90 (chín mươi) ngày kể từ ngày khách hàng thiết lập để sử dụng dịch vụ ngân hàng điện tử;

- Khách hàng nên tạo thói quen định kỳ thay đổi mật khẩu hoặc khi nghi ngờ bị lộ thông tin;
- Khách hàng không lưu tên đăng nhập và mật khẩu trên các trình duyệt hoặc lưu dưới bất kỳ hình thức nào để tránh lộ thông tin.

3. Giao dịch an toàn

- Khách hàng không nên dùng máy tính công cộng để truy cập, thực hiện giao dịch; không nên sử dụng mạng Wifi công cộng khi sử dụng dịch vụ ngân hàng trực tuyến;
- Khách hàng nên thoát khỏi hệ thống ứng dụng ngân hàng trực tuyến khi không sử dụng;
- Khách hàng nên cài đặt, sử dụng phần mềm diệt virus có bản quyền và được cập nhật mới nhất trên thiết bị cá nhân sử dụng để giao dịch ngân hàng điện tử;
- Khách hàng nên lựa chọn các giải pháp xác thực có mức độ an toàn, bảo mật phù hợp với nhu cầu của khách hàng về giá trị giao dịch thanh toán;
- Khách hàng không nên sử dụng các thiết bị đã bị phá khóa để tải và sử dụng phần mềm ngân hàng điện tử và ứng dụng phương thức xác thực;
- Cảnh báo một số các thủ đoạn gian lận thường gặp:
 - + Lừa khách hàng tự chuyển tiền;
 - + Đánh cắp thông tin khách hàng thông qua các website giả mạo/đường link lạ, ...
 - + Không truy cập vào các đường link lạ;
 - + Không cài đặt các phần mềm lạ không rõ nguồn gốc;
 - + Không cấp quyền trợ năng cho bất kỳ ứng dụng nào;
 - + Không cung cấp thông tin liên quan đến tài khoản ngân hàng điện tử: Tên đăng nhập, Mật khẩu, Mã OTP hay bất cứ thông tin bảo mật dịch vụ ngân hàng, thông tin cá nhân nào khác cho bất cứ ai, kể cả nhân viên ngân hàng.

4. Lưu ý về trình duyệt và thiết bị sử dụng

- Khách hàng chỉ đăng nhập dịch vụ Ngân hàng điện tử của NCB qua trang chủ: <https://www.ncb-bank.vn/> hoặc <https://www.ncb-bank.vn/IziBankBiz/Corp/dang-nhap> hoặc ứng dụng NCB Izi Mobiz tải từ kho ứng dụng chính thức của IOS hoặc Android. Tất cả các trang web khác yêu cầu Quý khách nhập thông tin đều là giả mạo.