HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN NGÂN HÀNG SỐ NEOONE

I. Nguyên tắc đảm bảo an toàn

Để đảm bảo an toàn khi giao dịch online trên NeoOne, Quý khách vui lòng thực hiện theo các nguyên tắc sau đây:

· Thiết lập mật khẩu, mã PIN smart OTP (mã PIN) theo đúng hướng dẫn khi đăng ký dịch vụ; không nên sử dụng thông tin cá nhân dễ đoán để làm mật khẩu; thay đổi mật khẩu, mã PIN thường xuyên (tối thiểu 12 tháng/lần); bảo vệ mật khẩu, mã PIN và không chia sẻ thiết bị lưu trữ các thông tin này.

· Tuyệt đối không cài đặt các phần mềm lạ, phần mềm không có bản quyền, phần mềm không rõ nguồn gốc.

· Chỉ đăng nhập qua các thiết bị đáng tin cậy. Không sử dụng các thiết bị di động đã bị phá khoá hoặc can thiệp hệ điều hành (root, jailbreak…) để sử dụng ứng dụng ngân hàng số.

· Không nên sử dụng mạng wifi công cộng khi sử dụng dịch vụ ngân hàng. Thoát khỏi dịch vụ ngân hàng số khi không sử dụng.

· Lựa chọn các hình thức xác nhận giao dịch có mức độ an toàn, bảo mật theo quy định và phù hợp với nhu cầu về hạn mức giao dịch.

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

· Thông báo ngay cho ngân hàng trong các trường hợp: phát hiện giao dịch bất thường; bị mất thiết bị (máy tính/smartphone/ tablet…); bị mất thiết bị tạo OTP; nghi ngờ bị tin tặc tấn công; nghi ngờ bị lừa đảo….

II. Cảnh báo các loại hình lừa đảo trực tuyến

Đối tượng Đối tượng lừa đảo sử dụng các thủ đoạn tinh vi để đánh cắp thông tin dịch vụ ngân hàng của khách hàng, từ đó truy cập dịch vụ và chiếm đoạt tiền trong tài khoản.

Chúng cũng có thể giả mạo cơ quan có thẩm quyền gửi các thông báo giả, đe dọa… để yêu cầu khách hàng cài đặt phầm mềm/ứng dụng giả mạo hoặc yêu cầu khách hàng tự chuyển tiền.

Một số thủ đoạn phổ biến hiện nay:
· Giả mạo cơ quan có thẩm quyền (công an, toà án, cơ quan thuế…) gửi đường link/website giả mạo dịch vụ công để khách hàng cài đặt các ứng dụng giả mạo (ứng dụng VneID, ứng dụng của Tổng cục thuế…), từ đó chiếm quyền điều khiển thiết bị, ngầm đánh cắp thông tin bảo mật dịch vụ ngân hàng và thực hiện hành vi chuyển tiền trong tài khoản của khách hàng.

· Giả mạo cơ quan có thẩm quyền (toà án, công an…) đe doạ khách hàng có liên quan đến các hành vi phạm pháp (gây tai nạn giao thông, liên quan đến đường dây rửa tiền, buôn lậu, nợ cước viễn thông quốc tế…) và yêu cầu khách hàng thực hiện theo hướng dẫn (mở tài khoản mới, cung cấp thông tin, cài đặt ứng dụng, chuyển tiền tới tài khoản chỉ định…).

· Giả mạo Website/Fanpage/Tin nhắn SMS của ngân hàng và gửi đường link giả mạo để khách hàng nhận thông tin.

· Giả mạo nhân viên ngân hàng liên hệ khách hàng đề nghị hỗ trợ (hỗ trợ giao dịch chuyển tiền bị lỗi, hỗ trợ xử lý tra soát…) sau đó yêu cầu khách hàng cung cấp các thông tin bảo mật để thực hiện hành vi chiếm đoạt tài sản.

· Giả mạo doanh nghiệp, tổ chức thông báo khách hàng trúng thưởng khuyến mại, nhận mã khuyến mại… và yêu cầu khách hàng cung cấp thông tin bảo mật dịch vụ ngân hàng hoặc chuyển tiền.

· Đánh cắp thông tin truy cập trên các nền tảng mạng xã hội (Facebook, Zalo…) của bạn bè, người thân của khách hàng, qua đó liên lạc với khách hàng để đề nghị chuyển tiền hỗ trợ, cho vay.

III. Các lưu ý cho khách hàng

· VCBNeo không gửi đường link đăng nhập dịch vụ ngân hàng số cho khách hàng dưới mọi hình thức, tất cả các đường link đăng nhập gửi đến khách hàng đều là giả mạo.

· VCBNeo không liên hệ yêu cầu khách hàng cung cấp thông tin bảo mật dưới mọi hình thức, mọi yêu cầu cung cấp thông tin bảo mật dịch vụ đều là giả mạo.

· Quý khách hãy nâng cao cảnh giác đối với các yêu cầu qua kênh trực tuyến và nền tảng mạng xã hội. Đồng thời, báo cho cơ quan Công an/Cơ quan chức năng nơi gần nhất nếu thấy dấu hiệu nghi ngờ.

IV. Khi xảy ra tình huống khẩn cấp

Trường hợp nghi ngờ hoặc phát hiện có dấu hiệu bị lừa đảo, bị tin tặc tấn công, Quý khách hãy thực hiện theo thứ tự ưu tiên như sau:

1. Khoá dịch vụ hoặc đổi mật khẩu ngay lập tức

- Khoá dịch vụ theo số Hotline 19001816.
- Đổi mật khẩu bằng cách vào mục Cài đặt chọn Đổi mật khẩu.

2. Liên hệ ngay tới ngân hàng

- Theo số Hotline 19001816, hoặc đến ngay các điểm giao dịch ngân hàng để được trợ giúp (trong giờ hành chính).

3. Khôi phục cài đặt gốc (Factory reset)

- Đối với thiết bị trường hợp phát hiện/nghi ngờ cài đặt ứng dụng giả mạo.

4. Trình báo với cơ quan công an nơi gần nhất.