NGÂN HÀNG NHÀ NƯỚC **VIỆT NAM**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 4893 /NHNN-TT	*Hà Nội, ngày 06 tháng 7 năm 2021*
V/v đảm bảo an ninh, an toàn trong hoạt động thanh toán	

Kính gửi:

- Các tổ chức cung ứng dịch vụ thanh toán;
- Hiệp hội Ngân hàng Việt Nam.

Qua theo dõi tình hình hoạt động thanh toán, Ngân hàng Nhà nước Việt Nam cảnh báo một số hiện tượng liên quan đến vấn đề an ninh, an toàn trong hoạt động thanh toán thời gian gần đây như sau:

- Đối tượng mạo danh nhân viên ngân hàng gọi điện thoại cho khách hàng với lý do hỗ trợ kiểm tra số dư và giao dịch của khách hàng. Theo đó, sau khi đọc tên khách hàng và 6 số đầu tiên của thẻ ghi nợ nội địa, đối tượng yêu cầu khách hàng đọc nốt dãy số còn lại trên thẻ để xác nhận khách hàng đúng là chủ thẻ; sau đó thông báo ngân hàng sẽ gửi tin nhắn cho khách hàng và yêu cầu khách hàng đọc mã 6 số trong tin nhắn (thực chất là OTP để thực hiện giao dịch thanh toán trực tuyến). Trường hợp khách hàng thực hiện theo yêu cầu của đối tượng thì có thể gây rủi ro mất tiền trong tài khoản thẻ của khách hàng.

- Đối tượng chuyển một khoản tiền nhỏ vào tài khoản của khách hàng, sau đó mạo danh ngân hàng gọi điện thoại hoặc gửi tin nhắn (hiển thị tên thương hiệu ngân hàng) cho khách hàng thông báo giao dịch chuyển tiền bị treo và yêu cầu khách hàng truy cập vào đường dẫn Internet (đường link) trong tin nhắn để tra soát giao dịch, xác nhận thông tin, mở khóa lệnh chuyển tiền… nhằm lừa đảo khách hàng cung cấp thông tin bảo mật của dịch vụ ngân hàng điện tử (như tên truy cập, mật khẩu, OTP), sau đó chiếm quyền kiểm soát tài khoản của khách hàng. Ngoài ra, các đối tượng lừa đảo còn lập trang web mạo danh ngân hàng để tiếp nhận và hỗ trợ giải đáp thắc mắc về sản phẩm dịch vụ của ngân hàng, nhằm thu thập thông tin cá nhân, lịch sử giao dịch và tài khoản ngân hàng.

- Đối tượng gửi thư điện tử giả mạo ngân hàng (thư điện tử có chứa tên ngân hàng và chữ ký thư điện tử của nhân viên ngân hàng) thông báo khách hàng nhận được một khoản tiền và yêu cầu khách hàng xác nhận giao dịch bằng cách truy cập vào tệp (file) hoặc đường link có chứa mã độc gửi kèm trong thư điện tử nhằm chiếm đoạt thông tin và tiền trong tài khoản của khách hàng.

- Khách hàng nhận được một khoản tiền chuyển vào tài khoản thanh toán tại ngân hàng với nội dung cho vay, sau đó đối tượng gọi điện cho khách hàng báo vừa chuyển nhầm và yêu cầu khách hàng chuyển trả lại tiền (tài khoản nhận tiền lúc này khác với tài khoản đã chuyển nhầm); sau một thời gian, người chủ

tài khoản chuyển nhầm sẽ đòi tiền khách hàng cùng với tiền lãi vay. Trong một số trường hợp, đối tượng giả danh nhân viên ngân hàng thông báo có người chuyển nhầm tiền vào tài khoản của khách hàng và hướng dẫn thủ tục hoàn trả, theo đó gửi đường link yêu cầu khách hàng điền thông tin cá nhân (bao gồm các thông tin bảo mật của dịch vụ ngân hàng điện tử), sau đó chiếm đoạt tiền trong tài khoản của khách hàng.

- Đối tượng gửi tin nhắn mạo danh thương hiệu ngân hàng đến khách hàng (tin nhắn này được nhận, lưu trong cùng mục với các tin nhắn của ngân hàng trên điện thoại di động của khách hàng) để thông báo tài khoản của khách hàng có dấu hiệu hoạt động bất thường và hướng dẫn khách hàng xác nhận thông tin, thay đổi mật khẩu... thông qua truy cập đường link giả mạo gửi kèm trong tin nhắn, qua đó lừa đảo khách hàng tiết lộ các thông tin bảo mật của dịch vụ ngân hàng điện tử (tên truy cập, mật khẩu, mã OTP) để sử dụng chiếm đoạt tiền trong tài khoản của khách hàng.

- Đối tượng mạo danh công ty tài chính mời khách hàng vay vốn, hướng dẫn khách hàng cài đặt ứng dụng trên điện thoại di động (như ứng dụng Auto Cash...) để giải ngân một khoản tiền "ảo" (không có thực) kèm theo việc hiển thị hợp đồng tín dụng với con dấu giả, chữ ký giả của người có thẩm quyền của công ty tài chính nhằm lừa đảo khách hàng chuyển khoản đặt cọc để chiếm đoạt.

- Đối tượng mạo danh nhân viên nhà mạng liên hệ và đề nghị hỗ trợ chuyển đổi sim 3G thành sim 4G qua điện thoại, theo đó đối tượng hướng dẫn cách nhắn tin theo cú pháp của nhà mạng để chuyển đổi nhưng thực tế đây là yêu cầu chuyển đổi từ sim 3G (do khách hàng sử dụng) lên sim 4G của đối tượng lừa đảo. Nếu khách hàng làm theo hướng dẫn, đối tượng sẽ chiếm đoạt được quyền sử dụng số điện thoại. Khi có được thông tin cá nhân và số điện thoại di động, đối tượng liên hệ nhà mạng với tư cách là chủ thuê bao di động để yêu cầu thay thế SIM với lý do bị mất thẻ SIM hoặc thẻ bị lỗi. Nhà cung cấp dịch vụ di động hủy SIM hiện có và phát hành SIM mới. *Trường hợp số điện thoại được khách hàng đăng ký sử dụng dịch vụ ngân hàng điện tử và nhận thông tin giao dịch, mã OTP* thì có thể gây rủi ro mất tiền trên tài khoản của khách hàng.

Để đảm bảo an ninh, an toàn trong hoạt động thanh toán, Ngân hàng Nhà nước Việt Nam đề nghị:

1. Các tổ chức cung ứng dịch vụ thanh toán chủ động nắm bắt, cập nhật các phương thức, thủ đoạn tội phạm nêu trên; đẩy mạnh công tác tuyên truyền, giáo dục kiến thức, kỹ năng giao dịch tài chính an toàn; kịp thời cảnh báo rủi ro trên các kênh thông tin liên quan nhằm giúp khách hàng nâng cao nhận thức về rủi ro, cảnh giác trước những thủ đoạn tội phạm mới và thực hiện giao dịch tài chính an toàn, đảm bảo an toàn tiền và tài sản của khách hàng.

2. Hiệp hội Ngân hàng Việt Nam tăng cường phối hợp, trao đổi thông tin giữa các ngân hàng thành viên để nắm bắt, cập nhật các phương thức, thủ đoạn tội phạm, đẩy mạnh công tác tuyên truyền, giáo dục kiến thức, kỹ năng giao dịch tài chính an toàn; tích cực nghiên cứu biện pháp phòng, chống các phương thức, thủ đoạn tội phạm có thể xảy ra để định hướng, hỗ trợ các ngân hàng thành viên triển khai thực hiện có hiệu quả./.

TL. THỐNG ĐỐC
KT. VỤ TRƯỞNG VỤ THANH TOÁN
PHÓ VỤ TRƯỞNG

Lê Anh Dũng

Nơi nhận:
- Như trên;
- PTĐ Nguyễn Kim Anh (để b/c);
- Vụ trưởng VTT (để b/c);
- Vụ Truyền thông (để p/hợp);
- NHNN chi nhánh tỉnh, thành phố (để p/hợp);
- Lưu: VP, TT (2b).