NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 9976 /NHNN-CNTT V/v bảo đảm an ninh, an toàn thông tin giai đoạn quyết toán năm 2023 và Tết Nguyên đán Giáp Thìn.	*Hà Nội, ngày 27 tháng 12 năm 2023*

Kính gửi:
- Các tổ chức tín dụng;
- Chi nhánh ngân hàng nước ngoài;
- Các tổ chức cung ứng dịch vụ trung gian thanh toán;
- Bảo hiểm tiền gửi Việt Nam;
- Công ty Cổ phần Thanh toán Quốc gia Việt Nam;
- Công ty Quản lý tài sản của các tổ chức tín dụng Việt Nam;
- Trung tâm Thông tin tín dụng Quốc gia Việt Nam;
- Công ty Cổ phần Thông tin tín dụng Việt Nam.

Trong năm 2023, tình hình an toàn thông tin trên thế giới và tại Việt Nam vẫn tiếp tục diễn biến phức tạp với số lượng các cuộc tấn công mạng, cài mã độc có xu hướng tăng cao, đặc biệt trong các dịp lễ, tết và các sự kiện quan trọng của đất nước.

Để chủ động phòng ngừa, xử lý hiệu quả các cuộc tấn công mạng và bảo đảm an ninh, an toàn thông tin cho các hệ thống thông tin của đơn vị cũng như cung cấp thông suốt, hiệu quả các dịch vụ thanh toán, trung gian thanh toán cho khách hàng và các nghiệp vụ ngân hàng trong giai đoạn quyết toán năm 2023 và Tết Nguyên đán Giáp Thìn năm 2024, Ngân hàng Nhà nước Việt Nam (NHNN) đề nghị các đơn vị triển khai thực hiện các nội dung sau:

1. Quán triệt và thực hiện nghiêm các quy định của Nhà nước và ngành Ngân hàng về bảo đảm an ninh, an toàn hệ thống thông tin ngành Ngân hàng. Nghiêm túc thực hiện các yêu cầu triển khai tại các công văn, thông báo về các chiến dịch tấn công mạng, các loại mã độc mới, các lỗ hổng an ninh bảo mật đối với hệ thống thông tin đã được NHNN (Cục Công nghệ thông tin) và các đơn vị chức năng cảnh báo.

2. Đánh giá, rà soát, tối ưu các hệ thống thông tin quan trọng của đơn vị (Core Banking, Internet Banking, Mobile Banking, hệ thống thanh toán thẻ, ATM, POS, hệ thống cung cấp dịch vụ trung gian thanh toán, các cổng, trang thông tin điện tử...), hạ tầng kết nối với các hệ thống thông tin phục vụ thanh toán, quyết toán của các đơn vị khác (như các hệ thống thanh toán, chuyển tiền điện tử qua Ngân hàng Nhà nước, NAPAS; các hệ thống thanh toán song phương; thanh toán quốc tế; hệ thống phối hợp thu Ngân sách Nhà nước,...).

3. Tăng cường các biện pháp chủ động giám sát, theo dõi hoạt động và nhật

ký (log) của các hệ thống thông tin nêu trên và hệ thống quan trọng khác, đồng thời triển khai các biện pháp kỹ thuật ở mức cao nhất để kịp thời phát hiện và xử lý sớm các cuộc tấn công có thể xảy ra. Tắt các dịch vụ không cần thiết ngoài giờ giao dịch và trong thời gian nghỉ lễ.

4. Rà soát, kiểm tra bảo đảm sẵn sàng các phương án, kịch bản ứng cứu sự cố và dự phòng thảm họa cho các hệ thống thông tin quan trọng, trong đó:

- Thực hiện đầy đủ công tác sao lưu dữ liệu, ứng dụng quan trọng theo quy định bảo đảm việc phục hồi hoạt động bình thường và toàn vẹn dữ liệu cho các hệ thống thông tin quan trọng trong mọi trường hợp. Dữ liệu sao lưu các hệ thống thông tin quan trọng phải được lưu trữ ra phương tiện lưu trữ ngoài và cất giữ bảo quản an toàn, tách biệt với khu vực lắp đặt hệ thống thông tin.

- Sẵn sàng phương án xử lý khi phát hiện hệ thống thông tin có dấu hiệu bị khai thác, tấn công mạng hoặc xảy ra sự cố ảnh hưởng đến hoạt động của hệ thống (như các sự cố lỗi hệ thống, quá tải,...).

5. Tăng cường công tác truyền thông đến nhân viên và khách hàng về các thủ đoạn, hình thức tấn công, lừa đảo của tội phạm mạng và các biện pháp bảo đảm an toàn thông tin trong quá trình quản lý, vận hành và sử dụng dịch vụ ngân hàng điện tử, thanh toán thẻ và dịch vụ trung gian thanh toán.

6. Cử cán bộ trực, ứng cứu và xử lý sự cố phát sinh (nếu có), bảo đảm an ninh, an toàn các hệ thống thông tin và dịch vụ cung cấp cho khách hàng trước, trong và sau thời gian nghỉ lễ; yêu cầu các đối tác đang cung cấp dịch vụ bảo hành, bảo trì hệ thống thông tin, dịch vụ giám sát an toàn thông tin mạng (nếu có) bố trí nhân lực sẵn sàng phối hợp xử lý sự cố phát sinh (nếu có). Trường hợp xảy ra sự cố hoặc có vấn đề phát sinh cần hỗ trợ xử lý, đề nghị liên hệ ngay với NHNN (Cục Công nghệ thông tin) qua Đầu mối thông báo, tiếp nhận và xử lý sự cố an toàn thông tin, số điện thoại đường dây nóng 0848.595.983, email: antt@sbv.gov.vn.

Căn cứ hướng dẫn trên đề nghị Thủ trưởng các đơn vị tổ chức thực hiện./.

Nơi nhận:
- Như trên;
- Thống đốc NHNN (để b/c);
- PTĐ Phạm Tiến Dũng (để b/c);
- Lưu: VP, CNTT (LTPThủy).

TL. THỐNG ĐỐC
KT. CỤC TRƯỞNG CỤC CÔNG NGHỆ THÔNG TIN
PHÓ CỤC TRƯỞNG

Lê Hoàng Chính Quang