NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 114 /NHNN-CNTT V/v bảo đảm an toàn thông tin mạng trong dịp Tết Nguyên đán 2023	*Hà Nội, ngày 09 tháng 01 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.

Tình hình an toàn thông tin trên thế giới và tại Việt Nam trong năm 2022 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. Theo thống kê từ Công ty an ninh mạng Viettel, các nguy cơ an ninh mạng trong năm 2022 chủ yếu đến từ các hình thức: tấn công lừa đảo giả mạo (phishing) tăng 35% so với năm 2021; tấn công qua lỗ hổng bảo mật, trong đó số lượng lỗ hổng bảo mật phát hiện tăng 15% so với năm 2021, lỗ hổng có mức độ Nghiêm trọng và Cao chiếm khoảng 50% tổng số lỗ hổng; các cuộc tấn công từ các nhóm APT, đặc biệt là Mustang Panda và Goblin Panda.

Để phòng ngừa, xử lý hiệu quả các cuộc tấn công mạng và bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của đơn vị cũng như các dịch vụ cung cấp cho khách hàng trên không gian mạng trong dịp Tết Nguyên đán 2023, Ngân hàng Nhà nước Việt Nam (NHNN) đề nghị các đơn vị triển khai thực hiện các nội dung sau 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 và các đơn vị chức năng cảnh báo.

2. Tăng cường các biện pháp giám sát, theo dõi hoạt động và nhật ký (log) của các hệ thống thông tin quan trọng như Corebanking, ATM, Internet Banking, Mobile Banking, các cổng, trang tin điện tử 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.

3. 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. Hoàn thành công tác sao lưu dữ liệu trước kỳ nghỉ lễ bảo đảm việc phục hồi khi cần thiết. Trong đó, 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.

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

5. Cử cán bộ trực, ứng cứu và xử lý sự cố trong trường hợp phát sinh, bảo đảm an ninh, an toàn các hệ thống thông tin và dịch vụ cung cấp cho khách hàng trong suốt thời gian nghỉ lễ; yêu cầu đơn vị, doanh nghiệp đang cung cấp dịch vụ giám sát an toàn thông tin mạng (nếu có) cam kết và bố trí lực lượng giám sát, bảo vệ các hệ thống. 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 triển khai./.

TL. THỐNG ĐỐC
CỤC TRƯỞNG CỤC CÔNG NGHỆ THÔNG TIN

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

Lê Mạnh Hùng