NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 35 /2018/TT-NHNN	*Hà Nội, ngày 24 tháng 12 năm 2018*

THÔNG TƯ

Sửa đổi, bổ sung một số điều của Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;

Căn cứ Luật các tổ chức tín dụng ngày 16 tháng 6 năm 2010 và Luật sửa đổi, bổ sung một số điều của Luật các tổ chức tín dụng ngày 20 tháng 11 năm 2017;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 16/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Căn cứ Nghị định số 35/2007/NĐ-CP ngày 08 tháng 3 năm 2007 của Chính phủ về giao dịch điện tử trong hoạt động ngân hàng;

Căn cứ Nghị định số 117/2018/NĐ-CP ngày 11 tháng 9 năm 2018 của Chính phủ quy định về việc giữ bí mật, cung cấp thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài;

Theo đề nghị của Cục trưởng Cục Công nghệ thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư sửa đổi, bổ sung một số điều của Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet (Thông tư 35/2016/TT-NHNN).

Điều 1. Sửa đổi, bổ sung một số điều của Thông tư 35/2016/TT-NHNN

1. Điều 3 được sửa đổi, bổ sung như sau:

"Điều 3. Nguyên tắc chung về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin cho việc cung cấp dịch vụ Internet Banking

1. Hệ thống Internet Banking là hệ thống thông tin quan trọng theo quy định của Ngân hàng Nhà nước về an toàn hệ thống thông tin trong hoạt động ngân hàng.

2. Đảm bảo tính bí mật, tính toàn vẹn của thông tin khách hàng; đảm bảo tính sẵn sàng của hệ thống Internet Banking để cung cấp dịch vụ một cách liên tục.

3. Các thông tin giao dịch của khách hàng được đánh giá mức độ rủi ro theo từng nhóm khách hàng, loại giao dịch, hạn mức giao dịch và trên cơ sở đó cung cấp biện pháp xác thực giao dịch phù hợp cho khách hàng lựa chọn. Biện pháp xác thực giao dịch phải đáp ứng:

a) Áp dụng tối thiểu biện pháp xác thực đa thành tố khi thay đổi thông tin định danh khách hàng;

b) Áp dụng các biện pháp xác thực cho từng nhóm khách hàng, loại giao dịch, hạn mức giao dịch theo quyết định của Thống đốc Ngân hàng Nhà nước trong từng thời kỳ;

c) Đối với giao dịch gồm nhiều bước, phải áp dụng tối thiểu biện pháp xác thực tại bước phê duyệt cuối cùng.

4. Thực hiện kiểm tra, đánh giá an ninh, bảo mật hệ thống Internet Banking theo định kỳ hàng năm.

5. Thường xuyên nhận dạng rủi ro, nguy cơ gây ra rủi ro và xác định nguyên nhân gây ra rủi ro, kịp thời có biện pháp phòng ngừa, kiểm soát và xử lý rủi ro trong cung cấp dịch vụ ngân hàng trên Internet.

6. Các trang thiết bị hạ tầng kỹ thuật công nghệ thông tin cung cấp dịch vụ Internet Banking phải có bản quyền, nguồn gốc, xuất xứ rõ ràng. Với các trang thiết bị sắp hết vòng đời sản phẩm và sẽ không được nhà sản xuất tiếp tục hỗ trợ, đơn vị phải có kế hoạch nâng cấp, thay thế theo thông báo của nhà sản xuất, bảo đảm các trang thiết bị hạ tầng có khả năng cài đặt phiên bản phần mềm mới.".

2. Khoản 3 Điều 4 được sửa đổi, bổ sung như sau:

"3. Thông tin khách hàng không được lưu trữ tại phân vùng kết nối Internet và phân vùng DMZ.".

3. Khoản 10 Điều 4 được sửa đổi, bổ sung như sau:

"10. Đường truyền kết nối Internet cung cấp dịch vụ phải bảo đảm tính sẵn sàng cao và khả năng cung cấp dịch vụ liên tục.".

4. Khoản 2 Điều 6 được sửa đổi, bổ sung như sau:

"2. Hệ thống Internet Banking phải có cơ sở dữ liệu dự phòng thảm họa có khả năng thay thế cơ sở dữ liệu chính và bảo đảm không mất dữ liệu giao dịch trực tuyến của khách hàng.".

5. Điểm c và điểm đ khoản 6 Điều 7 được sửa đổi, bổ sung như sau:

"c) Kiểm soát phiên giao dịch: hệ thống có cơ chế tự động ngắt phiên giao dịch khi người sử dụng không thao tác trong một khoảng thời gian do đơn vị quy định hoặc áp dụng các biện pháp bảo vệ khác;";

"đ) Đối với khách hàng là tổ chức, phần mềm ứng dụng được thiết kế để đảm bảo việc thực hiện giao dịch bao gồm tối thiểu hai bước: tạo, phê duyệt giao dịch và được thực hiện bởi những người khác nhau. Trong trường hợp khách hàng là tổ chức được pháp luật cho phép áp dụng chế độ kế toán đơn giản, việc thực hiện giao dịch tương tự như khách hàng cá nhân.".

6. Khoản 3 Điều 8 được sửa đổi, bổ sung như sau:

"3. Phần mềm ứng dụng phải xác thực người dùng khi truy cập và không có tính năng ghi nhớ mã khóa truy cập. Trường hợp xác thực sai liên tiếp quá số lần do đơn vị quy định, phần mềm ứng dụng phải tự động khoá tạm thời không cho người dùng tiếp tục sử dụng.".

7. Bổ sung điểm c vào khoản 1 Điều 9 như sau:

"c) Đối với việc truy cập hệ thống Internet Banking bằng trình duyệt, đơn vị phải có biện pháp chống đăng nhập tự động.".

8. Khoản 2 Điều 9 được sửa đổi, bổ sung như sau:

"2. Phần mềm ứng dụng Internet Banking phải có tính năng bắt buộc khách hàng thay đổi mã khóa bí mật ngay lần đăng nhập đầu tiên; khóa tài khoản truy cập trong trường hợp bị nhập sai mã khóa bí mật liên tiếp quá số lần do đơn vị quy định. Đơn vị chỉ mở khóa tài khoản khi khách hàng yêu cầu và phải xác thực khách hàng trước khi thực hiện mở khóa tài khoản, bảo đảm chống gian lận, giả mạo.".

9. Khoản 3 Điều 12 được sửa đổi, bổ sung như sau:

"3. Đơn vị phải thiết lập chính sách hạn chế truy cập Internet đối với các máy tính thực hiện quản trị, giám sát hệ thống Internet Banking. Trường hợp cần phải kết nối Internet để phục vụ công việc, đơn vị phải:

a) Đánh giá rủi ro cho việc kết nối Internet;

b) Áp dụng các biện pháp kiểm soát cho việc kết nối;

c) Phương án thực hiện phải được người có thẩm quyền tại đơn vị phê duyệt.".

10. Bổ sung khoản 6 vào Điều 13 như sau:

"6. Cập nhật thông tin các lỗ hổng bảo mật được công bố có liên quan đến phần mềm hệ thống, hệ quản trị cơ sở dữ liệu và phần mềm ứng dụng theo thông tin từ Hệ thống tính điểm lỗ hổng phổ biến (Common Vulnerability Scoring System version 3 – CVSS v3). Thực hiện triển khai cập nhật các bản vá bảo mật hoặc các biện pháp phòng ngừa kịp thời đáp ứng các tiêu chí sau:

a) Trong vòng 1 tháng sau khi công bố với lỗ hổng bảo mật được đánh giá ở mức nghiêm trọng (tương đương với CVSS v3 điểm từ 9.0 trở lên);

b) Trong vòng 2 tháng sau khi công bố với lỗ hổng bảo mật được đánh giá ở mức cao (tương đương với CVSS v3 điểm từ 7.0 đến 8.9);

c) Khoảng thời gian do đơn vị tự quyết định với lỗ hổng bảo mật được đánh giá ở mức trung bình hoặc thấp (tương đương với CVSS v3 điểm nhỏ hơn 7.0).".

11. Khoản 1 Điều 19 được sửa đổi, bổ sung như sau:

"1. Thông tin bí mật của khách hàng khi lưu trữ phải áp dụng các biện pháp mã hóa hoặc che dấu để đảm bảo tính bí mật."

Điều 2.

1. Bãi bỏ khoản 7 Điều 4 và khoản 1 Điều 10 Thông tư 35/2016/TT-NHNN.

2. Thay đổi cụm từ "Cục Công nghệ tin học" thành cụm từ "Cục Công nghệ thông tin" tại các Điều 20, 21 và 23 Thông tư 35/2016/TT-NHNN.

Điều 3. Trách nhiệm tổ chức thực hiện

Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước, Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương, Chủ tịch Hội đồng quản trị, Chủ tịch Hội đồng thành viên, Tổng giám đốc (Giám đốc) các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán chịu trách nhiệm tổ chức thực hiện Thông tư này.

Điều 4. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 7 năm 2019./.

Nơi nhận:
- Như Điều 3;
- Ban Lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu: VP, PC, CNTT (3 bản).

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Kim Anh