

Số: **04** /CT-BTTTT

Hà Nội, ngày **11** tháng **01** năm 2019

CHỈ THỊ
Về tăng cường phòng chống mã độc và
bảo vệ thông tin cá nhân trên không gian mạng

Hiện nay, các cơ quan, tổ chức, doanh nghiệp đang tích cực đẩy nhanh tiến trình ứng dụng công nghệ thông tin, chuyển đổi số, góp phần thúc đẩy phát triển nền kinh tế số, vì sự phát triển thịnh vượng của đất nước.

Song song với đó, thời gian gần đây, tình hình an toàn thông tin, đặc biệt là tình hình lây nhiễm mã độc, tấn công mạng gây lộ lọt thông tin cá nhân của người dùng trên không gian mạng đang diễn ra ngày càng phổ biến, gây thiệt hại cho các cơ quan, tổ chức, doanh nghiệp và người dùng, gây bức xúc trong dư luận, ảnh hưởng tiêu cực tới hình ảnh quốc gia.

Nhằm xử lý tình hình lây nhiễm mã độc; phòng, chống nguy cơ lộ lọt thông tin cá nhân, tăng cường bảo đảm an toàn thông tin trên không gian mạng, Bộ trưởng Bộ Thông tin và Truyền thông yêu cầu các cơ quan, đơn vị, doanh nghiệp thực hiện các quy định của pháp luật về an toàn thông tin, tập trung vào một số nhiệm vụ như sau:

1. Các doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet

a) Phát hiện, cảnh báo, khuyến cáo xử lý khi thiết bị của người dùng bị lây nhiễm mã độc, qua các kênh thông tin như: thư điện tử, điện thoại, thông báo trực tiếp khi thu cước dịch vụ, v.v...;

b) Tham gia các chiến dịch xử lý, bóc gỡ mã độc trên diện rộng do Cục An toàn thông tin phát động; phối hợp xử lý, bóc gỡ mã độc ra khỏi hệ thống thông tin trên phạm vi mạng lưới của mình theo yêu cầu của Cục An toàn thông tin;

c) Rà soát, đánh giá tổng thể về bảo vệ thông tin cá nhân nói riêng, công tác bảo đảm an toàn thông tin nói chung trong hoạt động của doanh nghiệp. Xây dựng, ban hành các quy chế, quy trình bảo vệ thông tin cá nhân. Hoạt động thu thập, lưu trữ, xử lý thông tin cá nhân của người dùng cần phải được áp dụng giải pháp kỹ thuật để chống lộ lọt thông tin, tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật bảo đảm an toàn thông tin;

d) Công bố quy trình thông báo, hướng dẫn, khuyến nghị xử lý khi xảy ra sự

cố lộ, lọt thông tin cá nhân của người dùng, trong đó, xác định rõ đầu mối, quy trình và trách nhiệm xử lý;

đ) Khắc phục các sự cố mất an toàn thông tin, nguy cơ, dấu hiệu lộ, lọt thông tin cá nhân của người dùng; kịp thời thông báo cho Cục An toàn thông tin và các cơ quan chức năng có thẩm quyền liên quan để phối hợp xử lý kịp thời các vấn đề phát sinh;

e) Rà soát, giám sát hoạt động của các tổ chức, doanh nghiệp cung cấp dịch vụ trên hạ tầng mạng của mình; xử lý các tổ chức, doanh nghiệp cung cấp dịch vụ có nội dung lừa đảo, thu thập trái phép thông tin cá nhân của người dùng hoặc phát tán mã độc, đồng thời báo cáo Bộ Thông tin và Truyền thông (Cục An toàn thông tin) để theo dõi và xử lý theo quy định của pháp luật;

g) Báo cáo việc triển khai theo yêu cầu của cơ quan nhà nước có thẩm quyền về việc ngăn chặn, xử lý hành vi phát tán mã độc và thu thập, lưu trữ, xử lý thông tin người dùng trái phép.

2. Các tổ chức tài chính, tín dụng; tổ chức, doanh nghiệp thiết lập mạng xã hội; doanh nghiệp cung cấp dịch vụ thương mại điện tử; các tổ chức, doanh nghiệp khác có hoạt động thu thập, lưu trữ, xử lý thông tin cá nhân

a) Triển khai các biện pháp quản lý và kỹ thuật bảo đảm an toàn thông tin cho hệ thống thông tin, phòng chống nguy cơ lây nhiễm mã độc; nguy cơ dẫn đến lộ, lọt thông tin cá nhân; tuân thủ các quy định về bảo vệ thông tin cá nhân theo quy định tại Mục 2, Chương II, Luật An toàn thông tin mạng;

b) Định kỳ kiểm tra, đánh giá an toàn hệ thống thông tin để phát hiện, xử lý bóc gỡ mã độc, tránh lộ, lọt thông tin cá nhân;

c) Cảnh báo, khuyến cáo người dùng khi có dấu hiệu lộ, lọt thông tin hoặc phát hiện đối tượng giả mạo dịch vụ của tổ chức, doanh nghiệp để lừa đảo; hướng dẫn người dùng cách xử lý và thông báo vi phạm khi phát hiện website giả mạo dịch vụ của mình để lừa đảo, thu thập thông tin cá nhân trái phép;

d) Các hoạt động thu thập, lưu trữ, xử lý thông tin cá nhân của người dùng cần phải được áp dụng giải pháp kỹ thuật để chống lộ lọt thông tin, tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật bảo đảm an toàn thông tin;

đ) Khắc phục các sự cố mất an toàn thông tin, nguy cơ, dấu hiệu lộ, lọt thông tin cá nhân của người dùng; kịp thời thông báo cho Cục An toàn thông tin và các cơ quan chức năng có thẩm quyền liên quan để phối hợp xử lý kịp thời các vấn đề phát sinh.



3. Cục An toàn thông tin

a) Chủ động rà quét, phát hiện mã độc, điểm yếu, lỗ hổng an toàn thông tin trên không gian mạng; kịp thời cảnh báo, tổ chức phát động và chỉ đạo, điều phối các doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet triển khai các chiến dịch xử lý, bóc gỡ mã độc trên diện rộng;

b) Cảnh báo, chia sẻ thông tin, hướng dẫn, hỗ trợ các bộ, ngành, địa phương xử lý bóc gỡ và ngăn chặn việc tái lây nhiễm mã độc trên hệ thống thông tin;

c) Giám sát, phát hiện và cảnh báo sớm cho cộng đồng nguy cơ, dấu hiệu của các cuộc tấn công mạng theo hình thức lừa đảo, giả mạo thu thập thông tin người dùng trái phép và tấn công lây nhiễm mã độc trên không gian mạng; xây dựng và tuyên truyền, phổ biến các tài liệu về quy định pháp luật, hướng dẫn ngăn chặn, xử lý bóc gỡ mã độc và phòng, chống lộ lọt thông tin cá nhân cho các cơ quan, tổ chức, cộng đồng;

d) Kiểm tra, đôn đốc, hướng dẫn các cơ quan, tổ chức, doanh nghiệp, cá nhân trong việc thực hiện các biện pháp bảo đảm an toàn thông tin, phòng, chống mã độc và bảo vệ thông tin cá nhân của người dùng trên không gian mạng;

đ) Thiết lập cổng thông tin điện tử cung cấp cho các cơ quan, tổ chức và người dùng thông tin về mã độc và công cụ miễn phí để rà quét, phát hiện, xử lý bóc gỡ mã độc; kênh thông tin trực tuyến để tiếp nhận kiến nghị, phản ánh của cơ quan, tổ chức, cá nhân liên quan đến việc lây nhiễm mã độc, mất an toàn thông tin cá nhân trên không gian mạng.

4. Cục Báo chí, Cục Phát thanh, truyền hình và Thông tin điện tử

Chỉ đạo các cơ quan thông tấn, báo chí và tổ chức, doanh nghiệp thiết lập trang thông tin điện tử tổng hợp, mạng xã hội tăng cường tuyên truyền, phổ biến luật pháp, cơ chế, chính sách, các thông tin liên quan tới việc ngăn chặn, xử lý mã độc và bảo vệ thông tin người dùng trên không gian mạng; thường xuyên cung cấp thông tin cảnh báo, khuyến cáo để người dùng cảnh giác với các loại mã độc, thông tin lừa đảo, thu thập trái phép thông tin cá nhân của người dùng. Phương thức, nội dung tuyên truyền, phổ biến cần sáng tạo, đơn giản, dễ hiểu và thu hút người đọc để công tác này đạt hiệu quả cao, rộng khắp tới toàn xã hội.

5. Thanh tra Bộ

a) Chủ trì, phối hợp với Cục An toàn Thông tin và các đơn vị liên quan tăng cường triển khai hoạt động thanh tra, kiểm tra và xử lý nghiêm các sai phạm có liên quan tới các hành vi vi phạm pháp luật về an toàn thông tin, phát tán mã độc, thu thập, lưu trữ, sử dụng trái phép thông tin cá nhân người dùng;

b) Hướng dẫn, chỉ đạo thanh tra chuyên ngành các Sở Thông tin và Truyền thông tiến hành thanh tra, xử phạt nghiêm đối với các hành vi vi phạm pháp luật về an toàn thông tin, phát tán mã độc, thu thập, lưu trữ, sử dụng trái phép, làm lộ, lọt thông tin cá nhân của người dùng hoặc chuyển hồ sơ sang cơ quan công an điều tra, xử lý vụ việc có dấu hiệu vi phạm hình sự.

6. Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương

a) Triển khai đồng bộ giải pháp kỹ thuật thực hiện giám sát an toàn thông tin tập trung cho các hệ thống thông tin của cơ quan nhà nước tại địa phương; đảm bảo có thể chia sẻ thông tin, dữ liệu thống kê tình hình tấn công mạng, lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Thông tin và Truyền thông và quy định của pháp luật;

b) Tăng cường hoạt động thanh tra, kiểm tra và xử lý nghiêm các hành vi phát tán mã độc, thu thập, lưu trữ, sử dụng trái phép, làm lộ, lọt thông tin cá nhân người dùng trên mạng thuộc địa bàn quản lý;

c) Chỉ đạo các cơ quan báo chí, đài phát thanh, truyền hình trên địa bàn tăng cường thời lượng phát sóng, bài viết tuyên truyền, phổ biến nâng cao nhận thức cho các tổ chức, người dân về các quy định của pháp luật liên quan đến bảo vệ thông tin cá nhân, đồng thời luôn cảnh giác, tự bảo vệ mình để tránh bị lợi dụng.

7. Hiệp hội An toàn thông tin Việt Nam

a) Phối hợp Cục An toàn thông tin chia sẻ thông tin để cảnh báo lây nhiễm mã độc, lộ lọt thông tin cá nhân của người dùng nhận được từ các tổ chức, doanh nghiệp viên Hiệp hội;

b) Tuyên truyền, đôn đốc, nhắc nhở doanh nghiệp viên tuân thủ các quy định của nhà nước về phòng chống mã độc, bảo vệ thông tin cá nhân của người dùng;

c) Tham gia cùng các cơ quan nhà nước và các tổ chức có liên quan xây dựng quy trình cảnh báo, hướng dẫn khắc phục sự cố an toàn thông tin liên quan tới mã độc; xây dựng các tiêu chuẩn, quy chuẩn bảo vệ thông tin người dùng.

8. Các cơ quan, đơn vị thuộc Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương, Đài phát thanh, truyền hình Trung ương và địa phương, các cơ quan thông tấn, báo chí, doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet, tổ chức tài chính, tín dụng, tổ chức, doanh nghiệp thiết lập mạng xã hội, doanh nghiệp cung cấp dịch vụ

thương mại điện tử, các tổ chức, doanh nghiệp khác có hoạt động thu thập, lưu trữ, xử lý thông tin cá nhân người dùng có trách nhiệm phối hợp quán triệt và thực hiện nghiêm túc Chỉ thị này.

Cục An toàn thông tin có trách nhiệm chủ trì, phối hợp với các đơn vị liên quan theo dõi, đôn đốc, kiểm tra việc thực hiện Chỉ thị này, định kỳ 6 tháng tổng hợp kết quả và báo cáo Bộ trưởng./.

Nơi nhận:

- Thủ tướng và các Phó Thủ tướng Chính phủ (để b/c);
- Sở TTTT các tỉnh, thành phố trực thuộc TW;
- Các hội, hiệp hội, doanh nghiệp hoạt động trong ngành TTTT;
- Các đài phát thanh, truyền hình, cơ quan báo chí;
- Các doanh nghiệp viễn thông;
- Các doanh nghiệp cung cấp dịch vụ Internet;
- Các tổ chức tài chính, tín dụng;
- Các tổ chức, doanh nghiệp thiết lập mạng xã hội;
- Các doanh nghiệp cung cấp dịch vụ thương mại điện tử;
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Công TTĐT của Bộ;
- Lưu: VT, CATT.

BỘ TRƯỞNG



Nguyễn Mạnh Hùng