

UBND TỈNH HÀ TĨNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:1000/STTTT-TTCNTT
V/v tuyên truyền, hướng dẫn
phòng chống mã độc

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Tĩnh, ngày 24 tháng 12 năm 2018

Kính gửi:

- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Ban Biên tập các cơ quan Báo chí địa phương;
- Văn phòng Đại diện, PVTT các Báo TW và tỉnh bạn trên địa bàn;
- Cổng thông tin điện tử của tỉnh;
- Phòng VH-TT, Đài TT-TH các huyện, thành phố, thị xã;
- Các doanh nghiệp: Viettel, Vinaphone, VNPT, FPT Hà Tĩnh

Thực hiện Kế hoạch số 256/KH-UBND ngày 03/8/2018 của Ủy ban nhân dân tỉnh về việc bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước tỉnh Hà Tĩnh giai đoạn 2018-2020; Sở Thông tin và Truyền thông đã xây dựng nội dung tuyên truyền, hướng dẫn các mối nguy hại của mã độc, cách phòng chống mã độc cho các cơ quan, tổ chức, cá nhân trên địa bàn tỉnh (*nội dung kèm theo và đăng tải trên chuyên mục “Thông tin- Tuyên truyền” trên Cổng Thông tin điện tử Sở Thông tin và Truyền thông*). Sở Thông tin và Truyền thông đề nghị quý cơ quan thực hiện một số nội dung sau:

1. Báo Hà Tĩnh, Đài Phát thanh và Truyền hình tỉnh, các Tạp chí trong tỉnh, Cổng thông tin điện tử tỉnh, các cơ quan báo chí Trung ương và tỉnh bạn hoạt động trên địa bàn tăng cường các bài viết tuyên truyền về các mối nguy hại của mã độc cũng như hướng dẫn cách phòng chống mã độc trên các phương tiện thông tin đại chúng.

2. Các sở, ban, ngành đoàn thể cấp tỉnh; UBND các huyện, thành phố, thị xã thực hiện đăng, phát nội dung về việc hướng dẫn các mối nguy hại của mã độc, cách phòng chống mã độc. Hướng dẫn cán bộ công chức, viên chức, người lao động thực hiện một số nội dung nhằm góp phần tuyên truyền phòng chống mã độc trong cơ quan, tổ chức, đơn vị mình.

3. Phòng Văn hóa - Thông tin, Đài Truyền thanh - Truyền hình các huyện, thành phố, thị xã phối hợp chỉ đạo, hướng dẫn các xã, phường, thị trấn đưa nội dung tuyên truyền phòng, chống mã độc trên hệ thống truyền thanh cơ sở.

4. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet tuyên truyền, phổ biến nâng cao nhận thức cho cán bộ và khách hàng của mình về các mối nguy hại của mã độc và phương thức phòng, chống mã độc.

5. Đề nghị quý cơ quan, đơn vị phối hợp tuyên truyền cho cán bộ, công chức, viên chức và người lao động biết nhằm nâng cao năng lực, phòng chống mã độc, cải thiện mức độ tin cậy của quốc gia trong hoạt động giao dịch điện tử, thúc đẩy phát triển kinh tế - xã hội, góp phần đảm bảo quốc phòng, an ninh./.

Nơi nhận:

- Như trên;
- UBND tỉnh (để b/c);
- UBND các huyện, TP, TX;
- Lãnh đạo Sở;
- Lưu: VT, TTCNTT&TT.

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC
(Đã ký)**

Bùi Đắc Thế

Thưa quý vị và các bạn!

Thời đại hiện nay, công nghệ thông tin đã và đang được ứng dụng vào mọi mặt đời sống, phục vụ phát triển kinh tế - xã hội, góp phần bảo đảm quốc phòng, an ninh của đất nước. Trong xu hướng của cuộc cách mạng công nghiệp lần thứ 4, sẽ ngày càng có nhiều thiết bị thông minh được kết nối mạng. Những thiết bị này khi bị lây nhiễm các loại phần mềm độc hại (gọi tắt là mã độc) sẽ gây mất an toàn thông tin, tiềm ẩn nhiều nguy cơ khó lường. Trong những năm 2016-2018, một số cuộc tấn công mạng sử dụng mã độc làm thiệt hại nghiêm trọng cho nhiều cơ quan, tổ chức ở Việt Nam.

Các cơ quan, tổ chức ở Việt Nam đã và đang thực hiện nhiều giải pháp khác nhau trong việc xử lý mã độc. Tuy nhiên, hiệu quả đạt được chưa cao, khả năng chia sẻ thông tin thấp. Thực trạng lây nhiễm mã độc tại Việt Nam hiện nay rất đáng báo động. Đặc biệt, nhiều trường hợp tấn công mã độc mà cơ quan chức năng không phản ứng kịp thời để phát hiện, phân tích và gỡ bỏ. Để nâng cao năng lực, phòng chống mã độc, cải thiện mức độ tin cậy của quốc gia trong hoạt động giao dịch, thúc đẩy phát triển kinh tế - xã hội, góp phần đảm bảo quốc phòng, an ninh; Sở Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, cá nhân trên địa bàn tỉnh cần chú ý một số nội dung sau:

1. Đối với các cơ quan, ban ngành, đoàn thể cần tăng cường sử dụng chữ ký số cho văn bản điện tử tại cơ quan, đơn vị, tổ chức trong phạm vi cơ quan, đơn vị, địa phương mình. Bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới.

2. Các cơ quan nhà nước và cá nhân, tổ chức trên địa bàn tỉnh khi mua sắm các thiết bị điện tử có kết nối Internet (như camera giám sát, router, modem DSL...) cần thực hiện rà soát, kiểm tra, đánh giá về an toàn thông tin; trước khi đưa vào sử dụng cần thiết lập cấu hình an toàn thông tin phù hợp với quy định, tuyệt đối không sử dụng cấu hình mặc định.

3. Các sở, ban, ngành, đoàn thể cấp tỉnh; UBND các huyện, thành phố, thị xã tổ chức theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin trong phạm vi cơ quan, đơn vị mình, báo cáo kịp thời về Sở Thông tin và Truyền thông - cơ quan thường trực ứng cứu sự cố mạng để có phương án xử lý.

4. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet cần xây dựng và công bố quy trình thông báo, hướng dẫn, khuyến nghị xử lý mã độc, trong đó, xác định rõ đầu mối, quy trình, trách nhiệm xử lý khi phát hiện ra mã độc thông thường, mã độc nguy hiểm hoặc khi có yêu cầu của cơ quan chức năng. Thường xuyên tổ chức tuyên truyền, phổ biến nâng cao nhận thức cho cán bộ và khách

hàng của mình về các mối nguy hại của mã độc và phương thức phòng, chống. Chủ động rà quét, xử lý, bóc gỡ mã độc đã theo dõi, phát hiện được; chủ trì bóc gỡ, ngăn chặn mã độc có nguồn gốc từ các hệ thống của người dùng trong mạng lưới của mình có dấu hiệu tấn công tới các hệ thống khác.

Thưa quý vị và các bạn!

Để hạn chế phòng tránh sự cố liên quan đến mã độc hại, giảm thiểu mức độ nghiêm trọng của sự cố, đề nghị các cơ quan, đơn vị, tổ chức hướng dẫn cho các cán bộ, nhân viên hiểu được các nguy cơ, cách thức phần mềm độc hại xâm nhập vào hệ thống, lây nhiễm, lây lan, các chính sách phòng chống mã độc cũng như thực hành thường xuyên các khuyến cáo để tránh sự cố phần mềm độc hại như sau:

- Không mở những thư điện tử hoặc tập tin có đính kèm từ những địa chỉ của người gửi không rõ ràng hoặc có dấu hiệu nghi ngờ.

- Không truy cập vào các popup trên trình duyệt mà cảm thấy nghi ngờ hoặc có dấu hiệu bất thường.

- Không truy cập vào những trang web có khả năng chứa nội dung độc hại.

- Không mở các tập tin với phần mở rộng có khả năng kết hợp với phần mềm độc hại (Ví dụ: .bat, .exe, .pif, .vbs...).

- Không được vô hiệu hoá các cơ chế kiểm soát an ninh (ví dụ như không được tắt phần mềm Anti-virus, phần mềm phát hiện gián điệp, tường lửa cá nhân).

- Không sử dụng những tài khoản có quyền quản trị cấp cao cho hoạt động thông thường.

- Không tải hoặc thực thi các ứng dụng từ các nguồn không tin cậy.

- Không sử dụng hoặc hạn chế việc sử dụng phần mềm không cần thiết, ví dụ như các ứng dụng, dịch vụ không cần thiết, các phần mềm được cung cấp bởi các tổ chức không rõ nguồn gốc.

- Luôn cập nhật phần mềm, các bản vá cho hệ điều hành.

- Khi nghi ngờ bị nhiễm mã độc, cần thông báo ngay cho cơ quan để báo cáo kịp thời về Sở Thông tin và Truyền thông - cơ quan thường trực ứng cứu sự cố mạng để có phương án xử lý.

Cảm ơn quý vị và các bạn đã quan tâm lắng nghe!