UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 678 /SGDĐT-VP

V/v tăng cường đảm bảo an toàn, an ninh thông tin mạng trong dịp Lễ 30/4 và 01/5 trong ngành giáo dục và đào tạo.

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

Quảng Ngãi, ngày 25 tháng 4 năm 2022

Kính gửi:
- Phòng Giáo dục và Đào tạo huyện, thị xã, thành phố;
- Trung tâm GDNN - GDTX huyện;
- Đơn vị trực thuộc Sở GDĐT.

Thực hiện Công văn số 1353/BTTTT-CATTT ngày 18/4/2022 của Bộ Thông tin và Truyền thông, ý kiến chỉ đạo của Chủ tịch UBND tỉnh tại Công văn số 1777/UBND-KGVX ngày 20/4/2022 về việc tăng cường đảm bảo an toàn thông tin mạng trong dịp Lễ 30/4 và 01/5, Công văn số 505/STTTT-BCVT&CNTT ngày 22/04/2022 của Sở Thông tin và Truyền thông về việc tăng cường bảo đảm công tác an toàn thông tin nhân dịp Lễ 30/4 và 01/5, Sở Giáo dục và Đào tạo yêu cầu thủ trưởng các đơn vị triển khai, thực hiện nội dung sau:

1. Tiếp tục phổ biến, quán triệt, thực hiện nghiêm túc các Nghị quyết, Chỉ thị của Đảng, chính sách pháp luật của nhà nước về an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước đến với toàn thể cán bộ quản lý, giáo viên, nhân viên và học sinh trong toàn ngành. Nâng cao cảnh giác đối với các hành vi tấn công, phá hoại hệ thống mạng, các cơ sở dữ liệu và sử dụng Internet gây mất ổn định chính trị - xã hội trên địa bàn tỉnh. Đẩy mạnh công tác thông tin, tuyên truyền nhằm nâng cao nhận thức cho cán bộ quản lý, giáo viên về vai trò của ứng dụng CNTT trong các hoạt động giáo dục.

2. Tăng cường triển khai các biện pháp quản lý và kỹ thuật nhằm đảm bảo an toàn thông tin cho hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, đơn vị. Theo dõi, giám sát, chủ động phát hiện sớm nguy cơ, dấu hiệu tấn công mạng, triển khai các giải pháp đảm bảo an toàn thông tin cho máy tính cá nhân của cơ quan, đơn vị mình.

3. Thực hiện các biện pháp đảm bảo an toàn, an ninh thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý theo hướng dẫn tại Công văn số 1353/BTTTT ngày 18/4/2022 của Bộ Thông tin và Truyền thông *(đính kèm Công văn này)*.

4. Chủ động theo dõi, kiểm tra, rà soát các lỗ hổng bảo mật trên các hệ thống thông tin, thiết bị mạng, máy chủ đã được cảnh báo để kịp thời cập nhật, xử lý, khắc phục triệt để các lỗ hổng bảo mật và triển khai các giải pháp phòng ngừa để tránh bị lợi dụng, khai thác tấn công vào các hệ thống; thực hiện sao lưu dữ liệu thường xuyên để đảm bảo an toàn dữ liệu cá nhân, đơn vị.

5. Triển khai các giải pháp đảm bảo an toàn thông tin cho máy tính, thiết bị di động cá nhân của cơ quan, đơn vị; các hoạt động lưu trữ, xử lý, truyền gửi thông tin cần phải được áp dụng giải pháp kỹ thuật để mã hóa, tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật đảm bảo an toàn thông tin.

6. Chỉ đạo, quán triệt công chức, viên chức, người lao động không sử dụng chung tài khoản, mật khẩu trên các ứng dụng với mật khẩu tài khoản thư điện tử; tuyệt đối không sử dụng thư công vụ của tỉnh để đăng ký vào các mạng xã hội, diễn đàn và các trang thông tin công cộng khác.

7. Phân công 01 lãnh đạo tại đơn vị phụ trách và cử 01 cán bộ, công chức, viên chức làm đầu mối theo dõi các sự cố bất thường xảy ra trên hệ thống thông tin của đơn vị.

Trong trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố đề nghị liên hệ các đầu mối kỹ thuật sau:

- Sở Thông tin và Truyền thông tỉnh Quảng Ngãi:

+ Ông Nguyễn Quốc Huy Hoàng, Trưởng Phòng Bưu chính - Viễn Thông và CNTT; Điện thoại: 0982.142.211.

+ Ông Nguyễn Công Nguyên, Chuyên viên Phòng Bưu chính - Viễn Thông và CNTT; Điện thoại: 0914.559.068.

+ Bà Phạm Thị Ngọc Yến, Trung tâm công nghệ Thông tin và Truyền thông Quảng Ngãi; Điện thoại: 0906.835.511.

- Sở Giáo dục và Đào tạo Quảng Ngãi

+ Ông Nguyễn Đức Huân, Phó Chánh văn phòng, Sở Giáo dục và Đào tạo, Điện thoại/Zalo: 0914121856; Email: ndhuan@quangngai.edu.vn

+ Ông Trần Văn Thuận, Chuyên viên Văn phòng Sở, Sở Giáo dục và Đào tạo, Điện thoại/Zalo: 0862575279; Email: tvthuan@quangngai.edu.vn

Đề nghị các đơn vị quan tâm triển khai thực hiện, nếu phát sinh vấn đề báo cáo về Văn phòng Sở Giáo dục và Đào tạo để theo dõi, tổng hợp, tham mưu chỉ đạo./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Nguyễn Ngọc Thái

BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:1353 /BTTTT-CATTT V/v tăng cường đảm bảo an toàn thông tin mạng trong dịp Lễ 30/4 và 01/5	*Hà Nội, ngày 18 tháng 04năm 2022*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, Tổng Công ty nhà nước;
- Các Tập đoàn, Tổng Công ty, Công ty cung cấp dịch vụ Internet, viễn thông;
- Các Tổ chức tài chính, Ngân hàng thương mại.

Nhằm phòng, chống nguy cơ mất an toàn thông tin mạng xảy ra trong thời gian diễn ra Lễ Giải phóng miền Nam, thống nhất đất nước 30/4 và Quốc tế lao động 01/5, Bộ Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, doanh nghiệp tăng cường triển khai công tác bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

1. Tăng cường triển khai hoạt động bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng, nhạy cảm trọng tâm là:

a) Phân công lực lượng tại chỗ triển khai trực giám sát, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin mạng 24/7.

b) Yêu cầu các đơn vị chuyên trách, đơn vị cung cấp dịch vụ an toàn, an ninh mạng (nếu có) củng cố và ưu tiên nguồn lực, nhân lực cho nhiệm vụ giám sát và bảo vệ các hệ thống thông tin.

c) Chủ động rà soát các lỗ hổng, điểm yếu trên các hệ thống thông tin thuộc phạm vi quản lý và triển khai các giải pháp phòng ngừa và khắc phục triệt để các lỗ hổng, điểm yếu đã được Cục An toàn thông tin, Bộ Thông tin và Truyền thông cảnh báo như: các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft từ tháng 01 đến tháng 4 năm 2022; lỗ hổng bảo mật Spring4Shell,...

d) Bảo đảm duy trì, kết nối, kịp thời chia sẻ thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

2. Các doanh nghiệp cung cấp dịch vụ viễn thông, internet; Các tổ chức, doanh nghiệp cung cấp nền tảng chuyển đổi số, nền tảng chống dịch Covid-19:

a) Triển khai các biện pháp kỹ thuật ở mức cao nhất nhằm phát hiện, chặn lọc, ngăn chặn hoạt động tấn công mạng, phát tán thông tin xấu độc, thông tin vi phạm pháp luật trên hệ thống thông tin, hạ tầng mạng lưới thuộc phạm vi quản lý.

b) Thực hiện nghiêm và kịp thời các biện pháp xử lý theo yêu cầu của Bộ Thông tin và Truyền thông và cơ quan chức năng có thẩm quyền.

3. Cử đầu mối tiếp nhận thông tin với Cục An toàn thông tin, Bộ Thông tin và Truyền thông.

Trong trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ với Cục An toàn thông tin, Bộ Thông tin và Truyền thông thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, email: ir@vncert.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0389942878, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Các Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các đơn vị chuyên trách về công nghệ thông tin, an toàn thông tin tại các bộ, ngành;
- Thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Lưu: VT, CATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng