UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 1981/SGDĐT-QLCLGDCNTT
V/v sự cố nhiễm mã độc và giải pháp phòng, chống

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

Quảng Ngãi, ngày 04 tháng 11 năm 2025

Kính gửi: Các đơn vị thuộc và trực thuộc Sở Giáo dục và Đào tạo

Theo nội dung thông báo của Công an tỉnh Quảng Ngãi tại Công văn số 3427/CAT-ANM ngày 03/11/2025 về việc thông báo sự cố nhiễm mã độc và giải pháp phòng, chống;

Hiện nay, trên mạng Internet đang phát tán các tệp có chứa mã độc có mức độ nguy hiểm rất nghiêm trọng, gồm: "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.rar"; "BÁO CÁO TÀI CHÍNH2.exe"; "THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe"; "CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe"; "HỖ TRỢ KÊ KHAI THUẾ.exe"; "CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.exe"; "MẪU GIẤY ỦY QUYỀN.exe"; "BIÊN BẢN BÁO CÁO QUÝ III.exe". Tin tặc lợi dụng sự kiện Đại hội Đảng để phát tán mã độc có thể nhằm chiếm quyền điều khiển, đánh cắp, phá hoại thông tin, tài liệu nội bộ của tổ chức, cá nhân; lợi dụng làm "bàn đạp" tấn công mạng các hệ thống thông tin quan trọng của cơ quan Đảng, Nhà nước hoặc thực hiện các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

Giám đốc Sở Giáo dục và Đào tạo yêu cầu các đơn vị thuộc và trực thuộc Sở thực hiện các nội dung sau:

1. Tổ chức, chỉ đạo các bộ phận, cán bộ, công chức, viên chức và người lao động rà soát từng thiết bị (máy tính cá nhân, máy tính dùng chung) tại đơn vị; nếu có lưu trữ, kích hoạt các tệp tin mã độc nêu trên, thực hiện cô lập thiết bị, thống kê gửi thông tin về Sở Giáo dục và Đào tạo (qua Phòng Quản lý chất lượng giáo dục và Công nghệ thông tin), Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để được hướng dẫn, hỗ trợ xử lý; yêu cầu cán bộ, công chức, viên chức và người lao động không lưu trữ, chia sẻ, đăng tải các tệp tin mã độc này trên môi trường mạng.

2. Tổ chức, chỉ đạo các bộ phận, cán bộ, công chức, viên chức và người lao động rà soát việc cài đặt phần mềm phòng chống mã độc BKAV Endpoint Client, EDP Viettel đã được cấp; đơn vị, cán bộ, công chức, viên chức và người lao động đã được cấp phần mềm phòng chống mã độc mà không cài đặt để xảy ra mất an toàn thông tin thì phải chịu trách nhiệm trước pháp luật theo quy định.

3. Sử dụng các giải pháp bảo đảm an toàn thông tin mạng đã triển khai quét toàn bộ ổ đĩa thiết bị nhằm loại bỏ các mã độc đã cài đặt; bật tính năng tường lửa trên thiết bị (Windows Defender Firewall) và tiếp tục theo dõi thiết bị.

4. Các đơn vị đã được bố trí thiết bị tường lửa nhanh chóng thực hiện chặn địa chỉ IP 27[.]124[.]9[.]13 máy chủ điều khiển từ xa của mã độc.

Quá trình thực hiện, nếu có khó khăn, vướng mắc, đề nghị liên hệ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (đồng chí Thượng úy Hoàng Gia Bảo, số điện thoại: 0916.401.448, email: hgbaopa05-ca@quangngai.gov.vn).

Yêu cầu Thủ trưởng các đơn vị khẩn trương triển khai, thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Các phòng thuộc Sở;
- Lưu: VT, QLCLGDCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Đoàn Thành Nhân