UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 3502 /SGDĐT-VP
V/v tăng cường phòng ngừa, ứng phó với mã độc tống tiền Trigona và The Gentlemen

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

Hưng Yên, ngày 28 tháng 9 năm 2026

Kính gửi:
- UBND các xã, phường trên địa bàn tỉnh Hưng Yên;
- Các cơ sở giáo dục mầm non, phổ thông, GDTX trên địa bàn tỉnh;

Căn cứ Công văn số 7597/CAT-ANM ngày 23/9/2026 của Công an tỉnh Hưng Yên về việc tăng cường phòng ngừa, ứng phó với mã độc tống tiền Trigona và The Gentlemen;

Thời gian gần đây, tình hình tấn công mạng sử dụng mã độc tống tiền (ransomware) tiếp tục diễn biến phức tạp, có xu hướng gia tăng về quy mô và tính chất nguy hiểm. Qua công tác nắm tình hình của Công an tỉnh, trên địa bàn đã ghi nhận trường hợp hệ thống thông tin, máy chủ có dấu hiệu bị tấn công, xâm nhập liên quan đến các dòng mã độc tống tiền nguy hiểm như Trigona và The Gentlemen. Các loại mã độc này có khả năng xâm nhập qua các cổng dịch vụ quản trị từ xa (RDP, VNC...), khai thác lỗ hổng bảo mật phần mềm, sau đó thực hiện mã hóa toàn bộ dữ liệu máy chủ/máy trạm, đòi tiền chuộc và đe dọa phát tán dữ liệu nhạy cảm, gây nguy cơ gián đoạn nghiêm trọng hoạt động của các cơ quan, đơn vị và nhà trường.

Để chủ động phòng ngừa, ngăn chặn triệt để nguy cơ tấn công mạng, bảo đảm an toàn hệ thống thông tin, bảo vệ Cơ sở dữ liệu ngành Giáo dục và Đào tạo (csdl.hungyen.edu.vn) và dữ liệu quản lý nhà trường, Giám đốc Sở Giáo dục và Đào tạo (GDĐT) yêu cầu các phòng thuộc Sở, các cơ sở giáo dục trực thuộc và đề nghị UBND các xã/phường phối hợp chỉ đạo thực hiện nghiêm các nội dung sau:

1. Tăng cường rà soát, kiểm tra và gia cố hạ tầng an toàn thông tin

- Rà soát máy chủ và máy trạm: Khẩn trương tiến hành rà soát toàn bộ hệ thống máy chủ, máy tính công vụ, thiết bị lưu trữ dữ liệu và hệ thống camera giám sát tại cơ quan Sở và các nhà trường.

- Tắt các cổng kết nối không an toàn: Kiểm tra, đóng ngay các cổng dịch vụ quản trị từ xa qua mạng Internet (như RDP - cổng 3389, VNC, SSH, Telnet...) hoặc chỉ cho phép truy cập qua mạng riêng ảo (VPN) bảo mật.

- Cập nhật bản vá bảo mật: Rà soát, cập nhật kịp thời các bản vá lỗi cho hệ điều hành Windows, Linux và các phần mềm ứng dụng chuyên ngành (SMAS, vnEdu, CSDL ngành, E-office...).

2. Triển khai đồng bộ giải pháp diệt mã độc và diệt virus chuyên dùng

- Cài đặt công cụ diệt mã độc: Quán triệt 100% các máy tính công vụ làm việc tại cơ quan Sở và bộ phận văn thư, tài chính, quản trị mạng tại các trường học cài đặt và vận hành thường xuyên công cụ phòng chống mã độc và giải pháp giám sát an toàn thông tin.

- Sử dụng phần mềm diệt virus bản quyền: Đảm bảo 100% máy tính công vụ được trang bị phần mềm diệt virus có bản quyền, kích hoạt chế độ tự động cập nhật mẫu nhận diện mã độc hằng ngày và quét định kỳ hệ thống.

3. Thực hiện quy trình sao lưu dữ liệu dự phòng độc lập (Offline Backup)

- Sao lưu dữ liệu quan trọng: Các nhà trường và phòng chuyên môn thực hiện sao lưu định kỳ (tối thiểu 01 lần/tuần) đối với các dữ liệu cốt lõi: hồ sơ học tịch học sinh, dữ liệu điểm số, Học bạ số, văn bằng chứng chỉ, hồ sơ cán bộ giáo viên, dữ liệu tài chính - kế toán và hồ sơ công việc.

- Lưu trữ cách ly an toàn: Dữ liệu sao lưu phải được lưu trữ trên các thiết bị độc lập (ổ cứng di động, thiết bị lưu trữ NAS...) và ngắt kết nối hoàn toàn với mạng Internet/LAN sau khi hoàn thành sao lưu để tránh bị mã độc tống tiền lây lan và mã hóa các bản sao lưu.

4. Nâng cao cảnh giác và kỹ năng an toàn thông tin cho CBQL, giáo viên, nhân viên

- Quản lý tài khoản nghiêm ngặt: Đổi mật khẩu tài khoản truy cập Hệ thống CSDL ngành, Hệ thống Quản lý văn bản E-office, Email công vụ theo định dạng mật khẩu mạnh (tối thiểu 8 ký tự gồm chữ hoa, chữ thường, số và ký tự đặc biệt). Nghiêm cấm tuyệt đối việc chia sẻ tài khoản hoặc sử dụng mật khẩu mặc định.

- Cảnh giác trước email/tin nhắn lạ: Tuyệt đối không mở các tệp tin đính kèm, không nhấp vào các đường link lạ gửi qua Email, Zalo, Facebook hoặc tin nhắn SMS không rõ nguồn gốc. Không tải về hoặc cài đặt các phần mềm không rõ bản quyền, phần mềm bẻ khóa (crack) trên máy tính công vụ.

- Kiểm soát thiết bị ngoại vi: Thực hiện rà quét virus kỹ lưỡng các thiết bị lưu trữ ngoại vi (USB, ổ cứng di động) trước khi kết nối vào máy tính công vụ.

5. Quy trình ứng phó và xử lý sự cố khẩn cấp

- Khi phát hiện máy tính hoặc hệ thống có dấu hiệu bị tấn công, xâm nhập, chạy chậm bất thường hoặc xuất hiện các thông báo đòi tiền chuộc liên quan đến mã độc Trigona, The Gentlemen:

1. Ngắt kết nối ngay lập tức: Lập tức ngắt kết nối mạng (rút dây mạng LAN, tắt Wi-Fi) đối với thiết bị bị ảnh hưởng để ngăn chặn mã độc lây lan sang các máy tính khác trong mạng nội bộ.

2. Giữ nguyên hiện trạng: Tuyệt đối không tắt máy, không tự ý khởi động lại, không xóa các tệp tin bị mã hóa hoặc nộp tiền chuộc cho tội phạm mạng.

3. Thông báo khẩn cấp: Kịp thời báo cáo về Sở Giáo dục và Đào tạo (qua Văn phòng Sở) và thông báo cho Công an tỉnh Hưng Yên (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - PA05) để phối hợp khoanh vùng, điều tra và xử lý sự cố theo đúng quy định.

Giám đốc Sở GDĐT yêu cầu Thủ trưởng các phòng thuộc Sở, Hiệu trưởng các cơ sở giáo dục nghiêm túc quán triệt và triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Công an tỉnh Hưng Yên (để p/h);
- Ban Giám đốc;
- Các đơn vị thuộc Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Đỗ Minh Trí