UBND TỈNH HÀ TĨNH **SỞ NGOẠI VỤ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1481 /SNgV-VP V/v tăng cường rà soát, xử lý lỗ hổng bảo mật, phòng ngừa mã độc và bảo đảm an toàn, an ninh mạng	*Hà Tĩnh, ngày 10 tháng 9 năm 2026*

Kính gửi: Các phòng và đơn vị thuộc Sở

Ngày 03/9/2026, Công an tỉnh có Văn bản số 3749/CAT-ANM về thông báo lỗ hổng bảo mật nghiêm trọng; tháng 8 năm 2026 trên không gian mạng xuất hiện nhiều chiến dịch tấn công mạng tinh vi và các lỗ hổng nghiêm trọng trên các phần mềm ứng dụng phổ biến, đặc biệt hệ thống quản trị mã độc tập trung ghi nhận một số loại mã độc nguy hiểm đang lây nhiễm, ảnh hưởng trực tiếp đến các cơ quan, đơn vị trên địa bàn tỉnh. Các loại virus, mã độc này có thể bị đối tượng tấn công lợi dụng để chiếm quyền điều khiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware); Giám đốc Sở đề nghị các phòng, đơn vị thực hiện một số nội dung sau:

1. Tăng cường cảnh giác trước các hình thức lừa đảo trên không gian mạng

Toàn thể công chức, viên chức và người lao động:

- Không truy cập các đường link lạ, đường link được gửi qua thư điện tử, SMS, Zalo, mạng xã hội hoặc các nền tảng trao đổi thông tin khác khi chưa xác định rõ nguồn gốc.

- Không tải, cài đặt hoặc chạy các phần mềm, tệp tin không rõ nguồn gốc, đặc biệt là các tệp có phần mở rộng .exe, .scr, .lnk, các tệp cài đặt được gửi qua USB hoặc các nền tảng trực tuyến.

- Không cung cấp tài khoản, mật khẩu, mã OTP, thông tin cá nhân hoặc thông tin liên quan đến hệ thống thông tin của cơ quan cho người khác qua điện thoại, thư điện tử hoặc mạng xã hội.

- Đối với các thông báo có nội dung yêu cầu xử lý gấp, xác thực tài khoản, thanh toán, chuyển tiền, cài đặt phần mềm hoặc truy cập đường link để xử lý công việc, phải kiểm tra, xác minh qua đầu mối chính thức trước khi thực hiện.

- Cảnh giác với các hình thức giả mạo cơ quan nhà nước, lãnh đạo, cán bộ chuyên môn hoặc các cơ quan, tổ chức có liên quan để yêu cầu cung cấp thông tin, chuyển tiền hoặc thực hiện các thao tác trên máy tính, điện thoại.

2. Rà soát, phòng ngừa và xử lý mã độc trên máy tính

Các phòng, đơn vị tổ chức rà soát toàn bộ máy tính, thiết bị công nghệ thông tin đang sử dụng, tập trung vào các nguy cơ:

- Mã độc lây nhiễm vào các tệp thực thi .exe, .dll, .scr và có khả năng lây lan sang các phần mềm, máy tính khác.

- Mã độc lây lan qua USB, ổ cứng di động và các thiết bị lưu trữ ngoài, đặc biệt là mã độc sử dụng tệp shortcut .lnk hoặc tệp giả danh phần mềm thông dụng.

- Mã độc giả mạo, đổi tên các tệp cài đặt phần mềm, phần mềm ký số, trình điều khiển máy in, máy scan hoặc các phần mềm nghiệp vụ.

- Các chương trình, phần mềm không rõ nguồn gốc hoặc không còn được sử dụng nhưng vẫn tồn tại trên máy tính

Thực hiện nghiêm các yêu cầu:

- Đối với máy trạm: Bảo đảm phần mềm phòng, chống mã độc Smart IR được cài đặt, hoạt động và cập nhật đầy đủ; không tự ý tắt, gỡ bỏ hoặc thay đổi cấu hình. Thường xuyên cập nhật hệ điều hành, trình duyệt và phần mềm; vô hiệu hóa AutoRun/AutoPlay và không tự ý cài đặt phần mềm không rõ nguồn gốc.

- Đối với USB, thiết bị lưu trữ ngoài: Hạn chế sử dụng thiết bị không rõ nguồn gốc; phải quét mã độc trước khi mở hoặc sao chép dữ liệu. Tuyệt đối không mở các tệp .lnk, .exe, .scr bất thường hoặc sử dụng bộ cài đặt không rõ nguồn gốc; không sao chép tệp thực thi từ máy nghi nhiễm sang thiết bị khác. Khi phát hiện dấu hiệu bất thường, ngừng sử dụng và báo ngay cán bộ phụ trách CNTT để xử lý.

3. Xử lý ngay khi phát hiện dấu hiệu nghi nhiễm mã độc

Khi máy tính có một trong các biểu hiện như chạy chậm bất thường, xuất hiện tệp lạ, tệp bị đổi tên, không mở được các chương trình, dữ liệu bị ẩn, xuất hiện shortcut bất thường hoặc phần mềm diệt virus cảnh báo mã độc, người sử dụng phải:

- Ngay lập tức ngắt kết nối mạng của máy tính nghi nhiễm để hạn chế mã độc tiếp tục phát tán hoặc kết nối đến máy chủ điều khiển.

- Rút USB, ổ cứng di động và các thiết bị lưu trữ ngoài đang kết nối với máy.

- Không tiếp tục đăng nhập các tài khoản quan trọng trên máy tính nghi nhiễm.

- Không tự ý sao chép dữ liệu từ máy nghi nhiễm sang máy tính khác.

- Không tự ý cài đặt các phần mềm diệt virus không rõ nguồn gốc hoặc thực hiện các biện pháp có thể làm mất dấu vết phục vụ kiểm tra, xử lý sự cố.

- Báo ngay cho Văn phòng Sở (đầu mối phụ trách công nghệ thông tin) để kiểm tra, cô lập và xử lý theo quy định.

- Trường hợp sự cố có dấu hiệu nghiêm trọng, ảnh hưởng đến nhiều máy tính, dữ liệu hoặc hệ thống thông tin của Sở, thực hiện báo cáo lãnh đạo Sở và phối hợp với cơ quan chuyên trách về an ninh mạng để được hỗ trợ.

4. Bảo vệ dữ liệu và tài khoản của cơ quan

Các phòng, đơn vị và cá nhân thực hiện nghiêm việc bảo vệ dữ liệu, tài khoản được giao:

- Không lưu trữ dữ liệu công việc quan trọng duy nhất trên máy tính cá nhân hoặc USB.

- Thực hiện sao lưu dữ liệu quan trọng theo quy định; ưu tiên sao lưu các tệp tài liệu như .docx, .xlsx, .pdf và các định dạng dữ liệu nghiệp vụ cần thiết.

- Không sao lưu các tệp thực thi .exe, .dll, .scr từ máy tính có dấu hiệu nghi nhiễm mã độc.

- Không sử dụng chung tài khoản, mật khẩu giữa nhiều người.

- Không lưu mật khẩu tài khoản công vụ tại những vị trí không an toàn hoặc chia sẻ mật khẩu qua các kênh không bảo đảm.

- Khi nhận được thư điện tử có tệp đính kèm hoặc đường link bất thường, phải kiểm tra kỹ địa chỉ người gửi, nội dung và nguồn gốc trước khi mở.

- Không tự ý đưa tài liệu, dữ liệu nội bộ, dữ liệu thuộc phạm vi bảo mật của cơ quan lên các nền tảng trực tuyến, công cụ AI, dịch vụ lưu trữ đám mây hoặc các hệ thống bên ngoài khi chưa được phép.

5. Rà soát các phần mềm và hệ thống thông tin đang sử dụng

Văn phòng Sở chủ trì, phối hợp với các phòng, đơn vị:

- Rà soát danh sách máy tính, thiết bị công nghệ thông tin đang kết nối mạng của Sở.

- Kiểm tra tình trạng cập nhật hệ điều hành, phần mềm bảo vệ máy trạm và các phần mềm nghiệp vụ.

- Rà soát các phần mềm không rõ nguồn gốc, phần mềm đã hết thời hạn hỗ trợ hoặc không còn nhu cầu sử dụng để kịp thời gỡ bỏ.

- Kiểm tra các thư mục dùng chung, thiết bị lưu trữ dùng chung và các tài khoản có quyền truy cập nhằm hạn chế nguy cơ lây nhiễm mã độc trong mạng nội bộ.

- Phối hợp với đơn vị cung cấp dịch vụ công nghệ thông tin để kiểm tra, xử lý khi phát hiện dấu hiệu bất thường.

6. Trách nhiệm của các phòng, đơn vị và cá nhân

- Văn phòng Sở là đơn vị đầu mối theo dõi, hướng dẫn, kiểm tra việc triển khai các nội dung bảo đảm an toàn thông tin; tổng hợp tình hình và tham mưu Lãnh đạo Sở xử lý các vấn đề phát sinh.

- Trưởng các phòng, đơn vị chịu trách nhiệm quán triệt nội dung Công văn này đến toàn thể công chức, viên chức, người lao động thuộc phạm vi quản lý; đồng thời chỉ đạo thực hiện nghiêm các biện pháp bảo đảm an toàn, an ninh mạng.

Đề nghị Trưởng các phòng, đơn vị và toàn thể công chức, viên chức, người lao động nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Công an tỉnh (để b/c);
- BGĐ Sở;
- Lưu: VT, VP$_3$.

Q. GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NGOẠI VỤ
TỈNH HÀ TĨNH

Ngô Thị Hoài Nam