UBND TỈNH HÀ TĨNH **SỞ TƯ PHÁP**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2377 /STP-VP V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 8/2026	*Hà Tĩnh, ngày 08 tháng 9 năm 2026*

Kính gửi: Các Phòng, Trung tâm thuộc Sở

Ngày 03/9/2026, Công an tỉnh có Văn bản số 3749/CAT-ANM về lỗ hổng bảo mật nghiêm trọng tháng 8/2026, cảnh báo về các thủ đoạn lừa đảo trên không gian mạng và một số mã độc nguy hiểm (Virus.Win32.Virut.ce, Virus.Win64.Moiva.a, Trojan.WinLNK.Runner, Virus.Win32.Renamer.j) đang lây nhiễm qua tệp tin thực thi và thiết bị lưu trữ USB, có nguy cơ chiếm quyền điều khiển hệ thống, đánh cắp, mã hóa dữ liệu đòi tiền chuộc (ransomware).

Để chủ động phòng ngừa, ngăn chặn nguy cơ mất an toàn thông tin, bảo vệ dữ liệu và hệ thống mạng của Sở, Giám đốc Sở yêu cầu các Phòng, Trung tâm thuộc Sở triển khai thực hiện các nội dung sau:

1. Phổ biến, quán triệt đến toàn thể công chức, viên chức, người lao động thuộc đơn vị nâng cao cảnh giác trước thủ đoạn giả danh cơ quan chức năng (Cảnh sát giao thông, cơ quan đăng kiểm...) gửi tin nhắn, gọi điện thông báo "phạt nguội" kèm đường link lạ như: .top, .vip, .cc hoặc file .apk để chiếm đoạt tài sản; tuyệt đối không truy cập đường link lạ, không cài đặt ứng dụng ngoài kho ứng dụng chính thống, không cung cấp mã OTP, thông tin tài khoản ngân hàng qua điện thoại, tin nhắn.

2. Rà soát việc đăng tải, chia sẻ thông tin, dữ liệu cá nhân (họ tên, số CCCD, ngày sinh, số điện thoại, địa chỉ...) của công chức, viên chức, người lao động và công dân, tổ chức có liên quan trên các nhóm, diễn đàn mạng xã hội; không đăng tải công khai danh sách, hồ sơ, kết quả có chứa thông tin định danh cá nhân khi chưa được che mờ hoặc ẩn các trường thông tin nhạy cảm.

3. Rà soát toàn bộ máy tính, máy trạm đang sử dụng; kịp thời phát hiện các dấu hiệu nhiễm mã độc (máy chạy chậm bất thường, ứng dụng .exe lỗi, không mở được...).

4. Trường hợp phát hiện dấu hiệu nhiễm mã độc, lập tức ngắt kết nối Internet, rút toàn bộ thiết bị lưu trữ ngoài (USB, ổ cứng di động) đang kết nối với máy; không tự ý diệt virus bằng phần mềm chạy trực tiếp trên hệ điều hành đang nhiễm; sử dụng đĩa cứu hộ (Rescue Disk) quét từ môi trường ngoài hệ điều hành; sao lưu các tệp tài liệu (.docx, .xlsx, .pdf...), tuyệt đối không sao lưu tệp .exe, trước khi định dạng lại ổ cứng và cài đặt lại hệ điều hành.

5. Tuyệt đối không mở các tệp shortcut (.lnk) lạ, không chạy các tệp cài đặt (.exe) không rõ nguồn gốc trên thiết bị lưu trữ ngoài; quét virus USB trước khi sử

dụng; vô hiệu hóa tính năng tự động chạy (AutoRun/AutoPlay) trên toàn bộ máy tính; chỉ tải phần mềm, bộ cài đặt, chữ ký số từ trang chính thống.

6. Duy trì thường xuyên phần mềm phòng, chống mã độc Smart IR trên toàn bộ máy tính thuộc Phòng, Trung tâm quản lý; trường hợp cần hỗ trợ cài đặt, cấp lại Key các đơn vị sự nghiệp thuộc Sở liên hệ đầu mối VNPT (Đồng chí Đặng Quốc Sinh, số điện thoại 0975357960).

(Cụ thể các nguy cơ tấn công, cảnh báo và giải pháp khắc phục có tại Văn bản số 3749/CAT-ANM được gửi kèm theo Văn bản này)

Đề nghị các Phòng, Trung tâm thuộc Sở tổ chức thực hiện kịp thời và có hiệu quả. Khi phát hiện dấu hiệu tấn công mạng, sự cố mất an toàn thông tin, kịp thời báo cáo Văn phòng Sở để phối hợp xử lý; trường hợp cần thiết liên hệ Phòng An ninh mạng và Phòng chống tội phạm sử dụng Công nghệ cao - Công an tỉnh (SĐT: 099.338.6777) để được hỗ trợ./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Lưu: VT, VP.

TL. GIÁM ĐỐC
Q. CHÁNH VĂN PHÒNG

CỘNG HÒA XHCN VIỆT NAM
SỞ TƯ PHÁP
TỈNH HÀ TĨNH

Thiều Thị Chiên