ỦY BAN NHÂN DÂN **XÃ ĐÔNG KINH**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /UBND-VHXH V/v triển khai các biện pháp phòng ngừa, ngăn chặn mã độc nguy hiểm lây nhiễm qua lỗ hổng bảo mật	*Đông Kinh, ngày tháng năm 2026*

Kính gửi:
- Các phòng chuyên môn thuộc UBND xã;
- Trung tâm Phục vụ hành chính công xã;
- Công an, quân sự xã;
- Các Trường học, Trạm Y tế trên địa bàn xã;
- Các thôn trên địa bàn xã.

Thực hiện Công văn số 5038/CAT-KTNV&NT ngày 09/11/2026 của Công an tỉnh Hà Tĩnh về việc cảnh báo mã độc nguy hiểm lây nhiễm qua lỗ hổng bảo mật; nhằm chủ động phòng ngừa, phát hiện, ngăn chặn nguy cơ mất an toàn thông tin, bảo vệ hệ thống máy tính, thiết bị điện tử và dữ liệu phục vụ hoạt động của các cơ quan, đơn vị trên địa bàn, UBND xã yêu cầu các ban, phòng, ngành, đơn vị liên quan triển khai thực hiện nghiêm túc một số nội dung sau:

1. Tăng cường công tác tuyên truyền, cảnh báo về nguy cơ mất an toàn thông tin

Phổ biến, quán triệt đến toàn thể cán bộ, công chức, viên chức, người lao động về nguy cơ lây nhiễm mã độc Backdoor.bot (các tệp có tên WinAlert.exe, Commgr.exe, winsysapp.exe) thông qua các lỗ hổng bảo mật, phần mềm không rõ nguồn gốc, tệp đính kèm email và thiết bị USB.

Chủ động nhận biết các dấu hiệu máy tính có nguy cơ nhiễm mã độc như: máy tính hoạt động chậm, treo bất thường; CPU, RAM tăng cao khi không sử dụng ứng dụng; xuất hiện tiến trình, tài khoản, dịch vụ hoặc chương trình tự khởi động không rõ nguồn gốc; máy tính tự động kết nối Internet hoặc có các kết nối mạng bất thường; phần mềm diệt virus, Windows Defender bị vô hiệu hóa hoặc thay đổi cấu hình.

2. Triển khai các biện pháp bảo đảm an toàn hệ thống thông tin

Rà soát toàn bộ máy tính, thiết bị công nghệ thông tin đang được sử dụng tại cơ quan, đơn vị; kiểm tra tình trạng hoạt động của hệ điều hành, phần mềm bảo mật và các dấu hiệu bất thường có nguy cơ nhiễm mã độc.

Thường xuyên cập nhật hệ điều hành Windows, các phần mềm ứng dụng và bản vá bảo mật mới nhất; ưu tiên thay thế, nâng cấp các máy tính sử dụng hệ điều hành đã hết thời gian hỗ trợ, không còn được cập nhật bản vá bảo mật.

Bật và duy trì hoạt động thường xuyên của phần mềm diệt virus, bảo đảm cơ sở dữ liệu nhận diện mã độc được cập nhật đầy đủ; không tự ý vô hiệu hóa hoặc thay đổi cấu hình các phần mềm bảo vệ máy tính.

Chỉ sử dụng hệ điều hành, phần mềm có bản quyền, nguồn gốc rõ ràng; không tải, cài đặt phần mềm crack, keygen, phần mềm kích hoạt Windows, Office không rõ nguồn gốc hoặc các tệp tin không được kiểm chứng an toàn.

Không mở các tệp đính kèm, đường dẫn đáng ngờ trong email, tin nhắn; thận trọng khi sử dụng thiết bị USB, ổ cứng di động và các thiết bị lưu trữ bên ngoài.

Thực hiện sao lưu dữ liệu quan trọng định kỳ, bảo đảm an toàn thông tin, dữ liệu của cơ quan, đơn vị; quản lý chặt chẽ tài khoản, mật khẩu truy cập các hệ thống thông tin dùng chung.

3. Biện pháp xử lý khi phát hiện dấu hiệu nhiễm mã độc

Khi phát hiện máy tính có dấu hiệu nhiễm mã độc hoặc hoạt động bất thường, các cơ quan, đơn vị cần khẩn trương thực hiện:

Ngắt kết nối máy tính nghi nhiễm mã độc khỏi hệ thống mạng nội bộ (LAN), mạng diện rộng (WAN) và Internet để hạn chế nguy cơ lây lan sang các thiết bị khác.

Không tiếp tục sử dụng máy tính nghi nhiễm để truy cập các hệ thống thông tin, phần mềm dùng chung hoặc thực hiện các giao dịch có liên quan đến dữ liệu của cơ quan, đơn vị.

Phối hợp với cán bộ phụ trách công nghệ thông tin để kiểm tra, rà quét, xử lý mã độc bằng các công cụ chuyên dụng như Microsoft Defender Offline, Kaspersky Virus Removal Tool và các giải pháp phù hợp.

Chủ động thay đổi mật khẩu các tài khoản đã đăng nhập trên máy tính nghi nhiễm; xóa dữ liệu lưu trữ trên trình duyệt web như lịch sử truy cập, mật khẩu đã lưu, cookie, cache sau khi bảo đảm an toàn và có phương án xử lý phù hợp.

Kịp thời báo cáo UBND xã (qua Phòng Văn hóa - Xã hội) để tổng hợp, phối hợp với Công an xã và cơ quan chuyên môn có thẩm quyền hướng dẫn xử lý; không tự ý khôi phục kết nối mạng khi chưa xác định được nguyên nhân và bảo đảm thiết bị đã an toàn.

4. Tổ chức thực hiện

Các ban, phòng, ngành thuộc UBND xã: Căn cứ chức năng, nhiệm vụ được giao, tổ chức triển khai thực hiện các nội dung nêu trên; chịu trách nhiệm kiểm tra, quản lý các thiết bị công nghệ thông tin được giao sử dụng, bảo đảm an toàn hệ thống và dữ liệu thuộc phạm vi quản lý.

Phòng Văn hóa - Xã hội: Chủ trì theo dõi, đôn đốc, hướng dẫn các cơ quan, đơn vị triển khai thực hiện; phối hợp với Công an xã và các đơn vị liên quan trong việc kiểm tra, xử lý các sự cố mất an toàn thông tin; tổng hợp tình hình, tham mưu UBND xã báo cáo cấp có thẩm quyền khi cần thiết.

Công an xã: Phối hợp tuyên truyền, cảnh báo các nguy cơ mất an toàn thông tin; hướng dẫn, phối hợp xử lý khi phát hiện dấu hiệu tấn công mạng, lây nhiễm mã độc hoặc nguy cơ lộ, mất dữ liệu, bảo đảm an ninh mạng và an toàn thông tin trên địa bàn.

Các trường học, trạm y tế và các đơn vị trên địa bàn: Chủ động rà soát, kiểm tra hệ thống máy tính, thiết bị công nghệ thông tin thuộc phạm vi quản lý; phổ biến, quán triệt đến cán bộ, viên chức, người lao động thực hiện nghiêm các biện pháp phòng ngừa, ngăn chặn mã độc.

Các thôn: Tuyên truyền, phổ biến các nội dung cảnh báo đến cán bộ thôn và các tổ chức có liên quan; chú trọng việc sử dụng an toàn máy tính, thiết bị kết nối Internet phục vụ hoạt động tại thôn.

UBND xã yêu cầu các ban, phòng, ngành, đơn vị nghiêm túc triển khai thực hiện. Trong quá trình thực hiện, nếu phát hiện dấu hiệu nhiễm mã độc, sự cố mất an toàn thông tin hoặc các vấn đề phát sinh, kịp thời thông tin về UBND xã (qua Phòng Văn hóa - Xã hội) để phối hợp xử lý, không để xảy ra tình trạng lây lan, ảnh hưởng đến hoạt động của cơ quan, đơn vị./.

Nơi nhận:
- Như trên;
- Lưu: VT, PVHXH.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Văn Hương