

**ỦY BAN NHÂN DÂN
PHƯỜNG MỸ HÀO**

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

Số: 1940 /UBND-VP

Mỹ Hào, ngày 23 tháng 7 năm 2026

V/v tăng cường bảo đảm an toàn
thông tin, an ninh mạng theo Báo cáo
số 5769/BC-CAT-ANM ngày 21/7/2026
của Công an tỉnh

Kính gửi:

- Các cơ quan, đơn vị thuộc UBND phường;
- Công an phường;
- Ban Chỉ huy Quân sự phường;
- Trung tâm Phục vụ hành chính công phường;
- Các tổ dân phố.

Thực hiện Báo cáo số 5769/BC-CAT-ANM ngày 21/7/2026 của Công an tỉnh Hưng Yên về tình hình an toàn thông tin tháng 7 năm 2026. Qua Báo cáo cho thấy tình hình an toàn thông tin, an ninh mạng tiếp tục diễn biến phức tạp; các đối tượng gia tăng sử dụng kỹ nghệ xã hội, phát tán mã độc thông qua tiện ích mở rộng trình duyệt (Chrome Extension), phần mềm giả mạo, trò chơi trực tuyến, website không rõ nguồn gốc nhằm đánh cắp thông tin xác thực, chiếm quyền tài khoản, phát tán mã độc và tấn công hệ thống thông tin. Đặc biệt, theo kết quả giám sát của Công an tỉnh, UBND phường Mỹ Hào phát sinh 395 lượt kết nối đến máy chủ chứa mã độc, liên quan 03 địa chỉ IP nội bộ, có dấu hiệu kết nối tới các hạ tầng chứa mã độc, website lừa đảo (phishing), Trojan-Spy.Win32.Zbot, Emotet, Gamarue và các hạ tầng độc hại khác. Điều này cho thấy nguy cơ mất an toàn thông tin đối với thiết bị đầu cuối vẫn hiện hữu, cần khẩn trương kiểm tra, xử lý và tăng cường các biện pháp phòng ngừa.

Để chủ động bảo đảm an toàn thông tin, an ninh mạng đối với hệ thống thông tin, thiết bị công nghệ thông tin phục vụ hoạt động quản lý nhà nước của UBND phường, UBND phường yêu cầu các cơ quan, đơn vị nghiêm túc triển khai thực hiện các nội dung sau:

1. Thủ trưởng các cơ quan, đơn vị thuộc UBND phường

- Chịu trách nhiệm trước UBND phường về công tác bảo đảm an toàn thông tin, an ninh mạng đối với toàn bộ hệ thống thông tin, máy tính, thiết bị công nghệ thông tin, tài khoản số và dữ liệu thuộc phạm vi quản lý.

- Tổ chức quán triệt, phổ biến đến toàn thể cán bộ, công chức, viên chức và người lao động thực hiện nghiêm các quy định của pháp luật, quy chế của cơ quan về bảo đảm an toàn thông tin, an ninh mạng; nâng cao cảnh giác trước các phương thức, thủ đoạn tấn công mạng mới, nhất là các hình thức lừa đảo qua thư điện tử, tin nhắn, website giả mạo, tiện ích mở rộng trình duyệt (Extension), phần mềm giả mạo, trò chơi trực tuyến và các ứng dụng, tệp tin không rõ nguồn gốc.

- Chỉ đạo rà soát toàn bộ máy tính, tài khoản và thiết bị thuộc phạm vi quản lý; kịp thời phát hiện, cô lập, xử lý các thiết bị có dấu hiệu lây nhiễm mã độc, phát sinh kết nối bất thường đến máy chủ độc hại hoặc có nguy cơ mất an toàn thông tin; phối hợp với Phòng Văn hóa - Xã hội và các cơ quan có liên quan để xử lý theo quy định.

- Không tự ý cài đặt, sử dụng phần mềm, tiện ích mở rộng trình duyệt, ứng dụng, launcher, plugin hoặc các chương trình không được phép; không truy cập các website độc hại, website có dấu hiệu lừa đảo; không mở các tệp đính kèm hoặc đường liên kết trong thư điện tử, tin nhắn khi chưa xác minh rõ nguồn gốc.

- Chỉ đạo cán bộ, công chức, viên chức sử dụng mật khẩu có độ mạnh theo quy định; thực hiện đổi mật khẩu ngay khi có dấu hiệu lộ lọt thông tin xác thực hoặc theo yêu cầu của cơ quan quản lý; ưu tiên áp dụng xác thực đa yếu tố (MFA) đối với các hệ thống thông tin có hỗ trợ; bảo đảm hệ điều hành, Microsoft Defender và các phần mềm đang sử dụng được cập nhật đầy đủ các bản vá bảo mật.

2. Phòng Văn hóa - Xã hội

- Chủ trì, phối hợp với Công an phường và các cơ quan, đơn vị có liên quan tổ chức rà soát, kiểm tra toàn bộ hệ thống máy tính, thiết bị đầu cuối, tài khoản và hệ thống thông tin thuộc phạm vi quản lý của UBND phường; kịp thời tham mưu UBND phường triển khai các biện pháp bảo đảm an toàn thông tin, an ninh mạng theo hướng dẫn của cơ quan có thẩm quyền.

- Chủ trì rà soát các máy tính được Công an tỉnh cảnh báo có dấu hiệu phát sinh kết nối đến máy chủ chứa mã độc; phối hợp với đơn vị hỗ trợ kỹ thuật xác minh nguyên nhân, thực hiện quét, xử lý mã độc, khắc phục các lỗ hổng, loại bỏ phần mềm độc hại, kiểm tra các phiên đăng nhập và thực hiện các biện pháp xử lý cần thiết đối với các tài khoản có nguy cơ bị lộ lọt thông tin xác thực.

- Hướng dẫn, đôn đốc các phòng chuyên môn, đơn vị trực thuộc kiểm tra, cập nhật hệ điều hành Windows, Microsoft Defender và các phần mềm đang sử dụng lên phiên bản mới nhất; bảo đảm 100% máy tính được cài đặt phần mềm phòng, chống mã độc, cập nhật đầy đủ các bản vá bảo mật; không để xảy ra tình trạng tắt hoặc vô hiệu hóa Microsoft Defender, Windows Update hoặc các cơ chế bảo vệ mặc định của hệ điều hành.

- Theo dõi, kiểm tra việc thực hiện công tác bảo đảm an toàn thông tin tại các phòng chuyên môn, đơn vị; kịp thời phát hiện, tổng hợp, báo cáo UBND phường các nguy cơ mất an toàn thông tin, phối hợp với Công an phường và cơ quan chuyên môn cấp trên xử lý các sự cố an toàn thông tin, an ninh mạng theo quy định.

3. Trung tâm Phục vụ hành chính công phường

- Chủ động rà soát toàn bộ máy tính, thiết bị công nghệ thông tin, thiết bị ký số, tài khoản công vụ và các tài khoản phục vụ tiếp nhận, giải quyết thủ tục hành chính thuộc phạm vi quản lý; bảo đảm hoạt động ổn định, liên tục, an toàn, không để xảy ra mất an toàn thông tin làm ảnh hưởng đến việc tiếp nhận, giải quyết thủ tục hành chính cho tổ chức, cá nhân.

- Thường xuyên kiểm tra việc sử dụng thư điện tử công vụ, tài khoản trên Hệ thống thông tin giải quyết thủ tục hành chính, tài khoản định danh điện tử và các tài khoản phục vụ thực hiện nhiệm vụ; kịp thời phát hiện, báo cáo và phối hợp xử lý các nguy cơ mất an toàn thông tin, nguy cơ lộ lọt thông tin xác thực hoặc phát sinh kết nối bất thường.

- Phối hợp với Phòng Văn hóa - Xã hội kiểm tra, cập nhật hệ điều hành Windows, Microsoft Defender, phần mềm phòng, chống mã độc và các bản vá bảo mật; thực hiện quét mã độc đối với các thiết bị thuộc phạm vi quản lý; kịp thời thay đổi mật khẩu đối với các tài khoản có nguy cơ bị lộ lọt thông tin xác thực theo quy định.

- Khi phát hiện dấu hiệu tấn công mạng, lây nhiễm mã độc hoặc sự cố an toàn thông tin, kịp thời thực hiện các biện pháp cần thiết để hạn chế ảnh hưởng, đồng thời báo cáo UBND phường (qua Phòng Văn hóa - Xã hội) và phối hợp với Công an phường, cơ quan chuyên môn để xử lý theo quy định.

4. Công an phường

- Phối hợp với Phòng Văn hóa - Xã hội và các cơ quan, đơn vị có liên quan triển khai các biện pháp bảo đảm an toàn thông tin, an ninh mạng; tăng cường nắm tình hình, kịp thời phát hiện, tiếp nhận thông tin về các nguy cơ, dấu hiệu tấn công mạng, lây nhiễm mã độc, lộ lọt dữ liệu hoặc các hành vi vi phạm pháp luật trên không gian mạng liên quan đến hệ thống thông tin của UBND phường.

- Kịp thời tiếp nhận, tổng hợp, báo cáo UBND phường và Công an cấp trên các vụ việc có dấu hiệu tấn công mạng, phát tán mã độc, chiếm quyền tài khoản, lộ lọt dữ liệu hoặc các sự cố an toàn thông tin khác; phối hợp triển khai các biện pháp ngăn chặn, xử lý theo quy định của pháp luật.

5. Cán bộ, công chức, viên chức và người lao động

- Thực hiện nghiêm các quy định của pháp luật, quy chế của cơ quan về bảo đảm an toàn thông tin, an ninh mạng; quản lý, sử dụng an toàn máy tính, thiết bị công nghệ thông tin, tài khoản công vụ và dữ liệu phục vụ công tác; không tự ý cài đặt phần mềm, tiện ích mở rộng trình duyệt (Extension), ứng dụng, plugin hoặc các chương trình không rõ nguồn gốc; không sử dụng tài khoản công vụ cho mục đích cá nhân; không lưu trữ, chia sẻ tài liệu công vụ trên các nền tảng hoặc dịch vụ không được cơ quan có thẩm quyền cho phép.

- Thường xuyên kiểm tra, cập nhật hệ điều hành Windows, Microsoft Defender và các phần mềm đang sử dụng; không truy cập các website có dấu hiệu độc hại, lừa đảo; không mở các tệp đính kèm, đường liên kết hoặc nhập thông tin xác thực khi chưa kiểm tra, xác minh nguồn gửi và tính hợp pháp của yêu cầu.

- Khi phát hiện thiết bị hoặc tài khoản có dấu hiệu bất thường như hoạt động không ổn định, xuất hiện phần mềm lạ, cảnh báo bảo mật, phát sinh kết nối bất thường, nghi ngờ lây nhiễm mã độc hoặc có dấu hiệu bị chiếm quyền tài khoản, phải ngừng thực hiện các giao dịch trên hệ thống, không tự ý xử lý hoặc can thiệp vào thiết bị, đồng thời báo cáo ngay Thủ trưởng đơn vị và Phòng Văn hóa - Xã hội để phối hợp với các cơ quan có liên quan kiểm tra, xử lý theo quy định.

6. Tổ chức thực hiện

- Các phòng chuyên môn, đơn vị thuộc UBND phường, Trung tâm Phục vụ hành chính công phường và các cơ quan, đơn vị có liên quan khẩn trương tổ chức triển khai thực hiện nghiêm các nội dung của Công văn này; chủ động rà soát, kiểm tra, xử lý các nguy cơ mất an toàn thông tin đối với hệ thống thông tin, máy tính, thiết bị công nghệ thông tin và tài khoản thuộc phạm vi quản lý.

- Giao Phòng Văn hóa - Xã hội theo dõi, đôn đốc, tổng hợp tình hình, kết quả thực hiện, tổng hợp, tham mưu UBND phường báo cáo cơ quan có thẩm quyền theo yêu cầu; kịp thời tham mưu UBND phường chỉ đạo xử lý các khó khăn, vướng mắc phát sinh trong quá trình triển khai.

- Các cơ quan, đơn vị báo cáo kết quả thực hiện về UBND phường (qua Phòng Văn hóa - Xã hội) theo yêu cầu hoặc khi có vụ việc phát sinh; trường hợp phát hiện dấu hiệu tấn công mạng, lây nhiễm mã độc, lộ lọt dữ liệu hoặc sự cố mất an toàn thông tin phải báo cáo ngay UBND phường, đồng thời phối hợp với Phòng Văn hóa - Xã hội, Công an phường và các cơ quan có liên quan để xử lý kịp thời theo quy định.

UBND phường yêu cầu Thủ trưởng các phòng cơ quan, đơn vị thuộc UBND phường và các tổ chức, cá nhân có liên quan nghiêm túc triển khai thực hiện. *hct*

Nơi nhận:

- Như trên;
- Thường trực Đảng ủy phường (b/c);
- Thường trực HĐND phường (b/c);
- Lãnh đạo UBND phường;
- Lưu: VT.



Trần Văn Tỉnh