UBND THÀNH PHỐ HẢI PHÒNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số:1173/SGDĐT-VP
V/v thông báo tình hình an toàn, an ninh mạng tháng 2/2026

Hải Phòng, ngày 03 *tháng* 3 *năm 2026*

Kính gửi:

- Ủy ban nhân dân xã, phường, đặc khu;
- Các cơ sở giáo dục.

Thực hiện chức năng quản lý nhà nước về giáo dục và đào tạo; căn cứ Thông báo số 2265/CAHP-ANM ngày 27/02/2026 của Công an thành phố Hải Phòng về việc thông báo tình hình an toàn, an ninh mạng trên địa bàn thành phố trong tháng 02/2026, Sở Giáo dục và Đào tạo đề nghị các đơn vị nghiêm túc triển khai một số nội dung sau:

1. Công tác quán triệt, tuyên truyền

- Tổ chức quán triệt nội dung Thông báo số 2265/CAHP-ANM đến toàn thể cán bộ quản lý, giáo viên, nhân viên, học sinh (sinh viên) phù hợp với từng cấp học.

- Tăng cường tuyên truyền, cảnh báo về tình trạng lừa đảo trực tuyến gia tăng, đặc biệt là các hình thức mạo danh fanpage, tour du lịch, dịch vụ sự kiện dịp đầu năm để chiếm đoạt tài sản và dữ liệu cá nhân.

- Nâng cao nhận thức về các nguy cơ mất an toàn thông tin từ lỗ hổng bảo mật nghiêm trọng được cơ quan chức năng cảnh báo trong tháng 02/2026.

2. Rà soát, bảo đảm an toàn hệ thống thông tin

- Rà soát toàn bộ hệ thống công nghệ thông tin của đơn vị (trang/cổng thông tin điện tử, phần mềm quản lý nhà trường, cơ sở dữ liệu ngành, hệ thống email công vụ…).

- Khẩn trương cập nhật các bản vá bảo mật đối với hệ điều hành Windows, Microsoft Office, trình duyệt Chrome và các phần mềm liên quan; đặc biệt lưu ý các lỗ hổng nghiêm trọng như:

+ Lỗ hổng trong thư viện vm2 của Node.js (CVE-2026-22709);

+ Lỗ hổng zero-day trong Microsoft Office (CVE-2026-21509);

+ Các lỗ hổng bảo mật trong Chrome (CVE-2026-2441 và các lỗ hổng liên quan JavaScript V8, libvpx);

+ Lỗ hổng trong ứng dụng Notepad tích hợp AI trên Windows 11 (CVE-2026-20841).

- Kiểm tra, cấu hình lại các biện pháp bảo mật: tường lửa, phần mềm phòng chống mã độc, hệ thống sao lưu dữ liệu.

3. Tăng cường quản lý tài khoản và dữ liệu

- Thực hiện nghiêm việc quản lý tài khoản truy cập hệ thống; định kỳ thay đổi mật khẩu, sử dụng mật khẩu mạnh và kích hoạt xác thực nhiều lớp (MFA) đối với tài khoản quản trị.

- Không cài đặt phần mềm, tiện ích mở rộng không rõ nguồn gốc; kiểm soát chặt chẽ quyền truy cập hệ thống.

- Bảo đảm an toàn dữ liệu cá nhân của cán bộ, giáo viên, học sinh theo quy định của pháp luật; không cung cấp thông tin, mã xác thực (OTP), tài khoản cho bên thứ ba.

- Thực hiện sao lưu dữ liệu định kỳ để phòng ngừa sự cố tấn công mã độc, mã hóa dữ liệu.

4. Công tác phối hợp và báo cáo

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, trình báo các đơn vị có thể liên hệ:

Công an thành phố Hải Phòng: Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao

+ Địa chỉ: Số 55 Bến Bính, Hồng Bàng, Hải Phòng

+ Điện thoại: 069.278.5415

Sở Giáo dục và Đào tạo Hải Phòng trân trọng thông báo./.

Nơi nhận:
- Như trên;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
THÀNH PHỐ HẢI PHÒNG

Uông Minh Long