

BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 926 /CAHP-ANM
V/v thông báo tình hình an toàn, an
ninh mạng tháng 01/2026

Hải Phòng, ngày 03 tháng 01 năm 2026

Kính gửi:

- Các cơ quan Đảng thành phố;
- Các cơ quan Trung ương đóng tại địa phương;
- Các Sở, ban, ngành;
- UBND các xã, phường, đặc khu;
- Các đơn vị sự nghiệp Thành phố;
- Các tổ chức chính trị, xã hội, doanh nghiệp.

Thực hiện nhiệm vụ quản lý nhà nước về an toàn, an ninh mạng trên địa bàn thành phố, Công an thành phố Hải Phòng thông báo về tình hình an ninh mạng và kết quả hoạt động của công tác giám sát an ninh mạng trong tháng 01/2026 như sau:

- Chính phủ đã ban hành Nghị định quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân. Nghị định gồm 5 chương, 42 điều và có hiệu lực kể từ ngày 01/01/2026, được ban hành nhằm cụ thể hóa phạm vi điều chỉnh, phân loại dữ liệu, bảo đảm quyền của chủ thể dữ liệu, từ đó hoàn thiện khung pháp lý và tăng cường hiệu lực quản lý nhà nước trong môi trường số Việt Nam.

- Các chuyên gia đã phát hiện một loại mã độc, được đặt tên là MacSync, được phân phối thông qua một ứng dụng swift ký và chứng thực để vượt qua kiểm soát của Apple, nhằm mục đích tải xuống và thực thi mã độc trong DMG giả trình cài đặt hợp pháp, sau đó thực thi kịch bản được mã hóa và sử dụng các biện pháp né tránh như kiểm tra kết nối, giới hạn thời gian và bỏ thuộc tính cách ly, đồng thời chuyển dữ liệu và có thể điều khiển từ xa.

- Trong tháng 01/2026, tin tặc đã thực hiện chiến dịch tấn công mạng sau:

+ Chiến dịch mang tên PCPCat, là một chiến dịch gián điệp tự động hóa, nhắm vào Next.js và React, gây nhiễu loạn hạ tầng đám mây và thu thập dữ liệu quy mô lớn. Tin tặc khai thác các lỗ hổng để xâm nhập 59.128 máy chủ trong dưới 48 giờ và tỉ lệ tấn công thành công lên tới 64,6%. Hiện nay, chiến dịch này vẫn đang được thực hiện và dự kiến sẽ có thể tiếp tục xâm nhập hơn 1,2 triệu máy chủ, do đó, nhà phát hành khuyến nghị người dùng tạm thời chặn IP C2 (67.217.57.240) và thay đổi ngay các thông tin đăng nhập bị lộ trong các tệp môi trường.

+ Chiến dịch tấn công mang tên Zoom Stealer, sử dụng tiện ích mở rộng trên trình duyệt Chrome, Firefox và Edge, thu thập dữ liệu liên quan đến các

cuộc họp trực tuyến như URL, ID, chủ đề, mô tả và mật khẩu nhúng, thông qua 18 tiện ích mở rộng. Các tiện ích này yêu cầu quyền truy cập vào 28 nền tảng hội họp, quyền tải xuống video, ghi âm và sau đó truyền dữ liệu được đánh cắp qua WebSocket tới tin tặc. Người dùng cần cảnh giác khi thấy tiện ích mở rộng yêu cầu cấp các quyền nhạy cảm trên.

+ Chiến dịch lừa đảo qua email lợi dụng tính năng gửi Email của Google Cloud Application Integration để phát tán thư giả mạo từ các tên miền thuộc Google, nhằm vượt qua cơ chế DMARC/SPF và nhắm vào hàng nghìn người dùng ở nhiều khu vực, bằng cách mô phỏng các thông báo doanh nghiệp và dẫn người dùng đến trang đăng nhập giả mạo của Microsoft. Người dùng cần cảnh giác, đánh giá kỹ càng email gửi đến trước khi thực hiện các hành động tiếp theo.

- Các nhà nghiên cứu về bảo mật đã phát hiện một tiện ích mở rộng của Chrome mang tên Phantom Shuttle trên Chrome Web Store giả mạo là các công cụ proxy nhằm chiếm đoạt lưu lượng truy cập và đánh cắp dữ liệu nhạy cảm. Người dùng cần nâng cao cảnh giác và cài đặt các tiện ích mở rộng từ các nguồn tin cậy.

- Trong tháng 01/2026, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Lỗ hổng React2Shell (CVE-2025-55182) là một lỗ hổng giải mã dữ liệu không an toàn trong giao thức Flight của React Server Components (RSC) được sử dụng bởi thư viện React và framework Next.js. Lỗ hổng này có thể bị khai thác từ xa mà không cần xác thực để thực thi mã JavaScript trên máy chủ và hiện đang bị khai thác trong thực tế.

+ Lỗ hổng CVE-2026-0625 cho phép thực thi lệnh từ xa trên các bộ định tuyến DSL D-Link cũ. Vấn đề bắt nguồn từ việc vô hiệu hóa không đúng cách các thành phần đặc biệt dùng trong Lệnh hệ điều hành và chèn lệnh qua dnscfg.cgi. Tin tặc có thể chèn và thực thi shell tùy ý mà không cần xác thực. Các mẫu bị khai thác cụ thể là DSL-2740R, DSL-2640B...

+ Microsoft đã phát hành bản vá bảo mật quy mô lớn, khắc phục tổng cộng 114 lỗ hổng trên nhiều thành phần cốt lõi của hệ sinh thái Windows và Microsoft 365. Trong đó, có 08 lỗ hổng nghiêm trọng và 106 lỗ hổng ở mức quan trọng, trải dài từ Windows NTFS, Desktop Window Manager tới các driver cấp thấp trong nhân hệ điều hành. Có 03 lỗ hổng Zero-day được vá, trong đó có 01 lỗ hổng đã được khai thác trong thực tế. Đây là bản vá cần được ưu tiên hàng đầu đối với các đội ngũ an ninh và quản trị hệ thống.

- Trong tháng 01/2026, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 773 thiết bị thuộc 82 tổ chức trên địa bàn thành phố Hải Phòng có tình trạng mất an ninh mạng, với tổng cộng 1614 mối đe dọa từ mã độc, link giả mạo, 14607 file độc hại. Qua công tác quản lý và nắm tình hình, Công an thành phố đã phát hiện tình trạng mất an ninh mạng, an toàn thông tin đối với Hệ

thống thông tin Công ty cổ phần Cảng Hải Phòng và Hệ thống thông tin Thành đoàn Hải Phòng; Công an thành phố đã thông báo và phối hợp với các đơn vị trên để làm rõ, kịp thời khắc phục.

Công an thành phố Hải Phòng đề nghị các sở, ban, ngành, tổ chức trên địa bàn thành phố chủ động cập nhật và nâng cấp giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin. Quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị liên hệ về Công an thành phố (*Qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; địa chỉ: Số 55 Bến Bính, Hồng Bàng, Hải Phòng; SĐT: 069.278.5415*) để được hướng dẫn, hỗ trợ./.

Nơi nhận:

- Như trên;
- Cục ANM và PCTPSCNC-BCA;
- Đ/c Giám đốc CATP (để báo cáo);
- Lưu VT; ANM(Đ4).

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**



Đại tá Lê Đức Thành

Phụ lục
DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN
(Kèm theo Công văn số **926** /CAHP-ANM ngày **3/2** /2026
của Công an thành phố)

1. Đơn vị nhận văn bản điện tử

STT	TÊN ĐƠN VỊ
Khối các cơ quan chính quyền thành phố	
1.	Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân thành phố
2.	Văn phòng Ủy ban nhân dân thành phố
3.	Sở Công Thương
4.	Sở Giáo dục và Đào tạo
5.	Sở Xây dựng
6.	Sở Tài chính
7.	Sở Khoa học và Công nghệ
8.	Sở Nội vụ
9.	Sở Ngoại vụ
10.	Sở Văn hóa, Thể thao và Du lịch
11.	Sở Nông nghiệp và Môi trường
12.	Sở Tư pháp
13.	Sở Y tế
14.	Ban Quản lý Khu kinh tế
15.	Thanh tra thành phố
16.	UBND các xã, phường, đặc khu (114 xã phường)
Khối các cơ quan Trung ương đóng trên địa bàn thành phố	
1.	Bảo hiểm xã hội thành phố Hải Phòng
2.	Bộ Chỉ huy Quân sự thành phố
3.	Ngân hàng nhà nước Khu vực 6
4.	Thuế thành phố Hải Phòng

5.	Chi cục Hải quan khu vực III
6.	Thống kê thành phố Hải Phòng
7.	Thi hành án dân sự thành phố Hải Phòng
8.	Tòa án nhân dân thành phố
9.	Kho bạc Nhà nước khu vực III
Khối các cơ quan Đảng thành phố	
1.	Văn phòng Thành ủy
2.	Ban Nội chính Thành ủy
3.	Ban Tuyên giáo và Dân vận Thành ủy
4.	Ban Tổ chức Thành ủy
5.	Ủy ban kiểm tra Thành ủy
6.	Đảng ủy các cơ quan Đảng thành phố
7.	Đảng ủy Ủy ban nhân dân thành phố
8.	Báo và phát thanh, truyền hình Hải Phòng
Khối các đơn vị sự nghiệp thuộc Ủy ban nhân dân thành phố	
1.	Vườn Quốc gia Cát Bà
2.	Trường Đại học Hải Phòng
3.	Trường Cao đẳng Kỹ thuật Hải Phòng
4.	Trường Cao đẳng Y tế Hải Phòng
5.	Trường Cao đẳng Kinh tế Hải Phòng
Tổ chức chính trị, xã hội	
1.	Ủy ban Mặt trận Tổ quốc Việt Nam thành phố
2.	Liên đoàn Lao động thành phố
3.	Đoàn Thanh niên Cộng sản Hồ Chí Minh thành phố
4.	Hội Nông dân thành phố
5.	Hội Cựu chiến binh thành phố

6.	Hội Liên hiệp Phụ nữ thành phố
7.	Liên minh Hợp tác xã thành phố
8.	Liên hiệp các Hội Khoa học và Kỹ thuật thành phố
9.	Hội Chữ thập đỏ thành phố

2. Đơn vị nhận bản cứng

1.	Công ty TNHH MTV điện lực Hải Phòng Số 9 Trần Hưng Đạo, Hồng Bàng, Hải Phòng
2.	Cảng hàng không quốc tế Cát Bi Lê Hồng Phong, Phường Hải An, Thành phố Hải Phòng
3.	Công ty cổ phần cấp nước Hải Phòng Số 54 Đinh Tiên Hoàng, Hồng Bàng, Hải Phòng
4.	Công ty cổ phần Cảng Hải Phòng Số 8A đường Trần Phú, Phường Ngô Quyền, Hải Phòng
5.	Viettel Hải Phòng Tòa Nhà Viettel, Đ. Lê Hồng Phong, Hải An, Hải Phòng
6.	Viễn thông Hải Phòng Lô C6 Khu Trung tâm hành chính quận Hải An, đường Lê Hồng Ph, Hải An, Hải Phòng
7.	Viện kiểm sát nhân dân thành phố Lê Hồng Phong, Hải An, Hải Phòng
8.	Trường Đại học Y Dược Hải Phòng 72A Nguyễn Bình Khiêm, Gia Viên, Hải Phòng
9.	MobiFone Hải Phòng 4 P. Trần Hưng Đạo, Hồng Bàng, Hải Phòng
10.	Công ty Cổ phần CMC Hải Phòng Toà nhà TD Business Center, Lô 20A Lê Hồng Phong, Gia Viên, Hải Phòng
11.	Chi Nhánh Hải Phòng - Công ty Cổ phần Viễn Thông FPT Thửa đất số 1, 2020 tổ 19, Lê Chân, Hải Phòng