

Số: /SGDDT-VP

Hải Phòng, ngày tháng năm 2025

V/v tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao, trên không gian mạng

Kính gửi:

- Trưởng phòng CMNV cơ quan Sở;
- Trưởng phòng GDĐT quận, huyện;
- Hiệu trưởng trường THPT, PT nhiều cấp;
- Giám đốc trung tâm GDNN-GDTX quận huyện;
- Thủ trưởng các đơn vị trực thuộc.

Thực hiện chỉ đạo của Ủy ban nhân dân thành phố tại Văn bản số 36/UBND-NCKTGS ngày 07/01/2025 về việc tăng cường phòng ngừa, xử lý hoạt động lừa đảo chiếm đoạt tài sản sử dụng công nghệ cao trên không gian mạng (gửi kèm theo).

Sở GDĐT đề nghị Thủ trưởng các đơn vị tăng cường triển khai công tác bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

a) Tổ chức các hoạt động tuyên truyền, nâng cao nhận thức kỹ năng cơ bản về an toàn thông tin mạng; Nhận biết, cảnh giác trước thông tin xấu độc, tin giả, thông tin xuyên tạc, chống phá, chính sách của Đảng và Nhà nước; Phòng, chống lừa đảo trên không gian mạng cho toàn thể cán bộ, giáo viên, nhân viên, học sinh và người lao động của đơn vị quản lý.

b) Rà soát các hệ thống thông tin, bảo đảm các hệ thống thông tin được triển khai đầy đủ các biện pháp bảo vệ theo cấp độ an toàn. Chủ động rà soát, xử lý, triển khai các giải pháp nhằm khắc phục triệt để các lỗ hổng an toàn thông tin mạng, đặc biệt là các lỗ hổng đã được Sở Thông tin và Truyền thông cảnh báo và chủ động thực hiện sẵn lòng mỗi nguy hại tiềm ẩn trong hệ thống hoặc tại địa chỉ <https://khonggianmang.vn/canhbaoattt/>, Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRlab.vn) và từ các cơ quan, tổ chức liên quan cung cấp.

c) Tổ chức lực lượng tại chỗ trực giám sát, hỗ trợ, ứng cứu và khắc phục sự cố an toàn thông tin mạng 24/7; Chủ động theo dõi thường xuyên, liên tục các hệ thống giám sát an toàn thông tin tập trung, hệ thống phòng, chống mã độc tập trung đảm bảo xử lý, khắc phục kịp thời tấn công mạng, cảnh báo mã độc được xác minh.

d) Rà soát, kiểm tra và bóc gỡ các phần mềm độc hại cho toàn bộ máy chủ, máy trạm trong hệ thống mạng. Trong đó, cần ưu tiên các hệ thống tin có địa chỉ IP nằm trong Danh sách IP mạng Botnet được Sở GDĐT, Sở Thông tin và Truyền thông cảnh báo hàng tháng hoặc đột xuất.

d) Khi gặp sự cố hoặc có vấn đề phát sinh, cần hỗ trợ xử lý, đề nghị liên hệ ngay với Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông (Cục An toàn thông tin) qua các đầu mối sau đây:

- Phòng An toàn hệ thống thông tin, số điện thoại trực đường dây nóng hỗ trợ tổng thể các giải pháp an toàn thông tin 0888.133.359, thư điện tử: athttt@mic.gov.vn.

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC): điện thoại (024) 3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, email: ir@vncert.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: (024) 3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 033.6666.905, thư điện tử: ais@mic.gov.vn.

- Sở Thông tin và Truyền thông: ông Nguyễn Đông Huy (Phó Giám đốc Trung tâm Thông tin và Truyền thông, số điện thoại 0984.462472)

- Sở GDĐT: ông Trần Tiến Chinh, Chánh Văn phòng Sở, số điện thoại 0914.463645

Sở GDĐT đề nghị Thủ trưởng các đơn vị chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- Sở TTTT (để p/h);
- Lưu: VT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Phạm Quốc Hiệu