ỦY BAN NHÂN DÂN HUYỆN THỦY NGUYÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 4053/UBND-VH&TT V/v tăng cường công tác bảo đảm an toàn, an ninh mạng	*Thủy Nguyên, ngày 27 tháng 11 năm 2023*

Kính gửi:
- Các phòng, ban, cơ quan, đơn vị, trường học;
- Ủy ban nhân dân các xã, thị trấn.

Thời gian vừa qua trên địa bàn thành phố xuất hiện trang thông tin điện tử, trang mạng xã hội của một số sở, ngành bị tấn công chiếm quyền điều khiển dẫn đến nguy cơ mất an toàn, an ninh mạng, ảnh hưởng xấu đến tình hình an ninh chính trị trên địa bàn thành phố.

Để bảo đảm an toàn, an ninh mạng đối với các kênh cung cấp thông tin trên môi trường mạng (trang/cổng thông tin điện tử, trang mạng xã hội, thư điện tử...), Ủy ban nhân dân huyện yêu cầu các phòng, ban, cơ quan, đơn vị, Ủy ban nhân dân các xã, thị trấn thực hiện một số nội dung sau:

1. Rà soát thống kê các kênh cung cấp thông tin trên môi trường mạng (trang/cổng thông tin điện tử, trang mạng xã hội, thư điện tử...) do đơn vị quản lý, quản trị, vận hành để triển khai các biện pháp bảo mật, bảo đảm an ninh an toàn. Đối với các trang thông tin điện tử, trang mạng xã hội hiện nay đơn vị không còn sử dụng thì tiến hành khóa, gỡ, xóa.

2. Trong quá trình sử dụng, quản trị trang thông tin điện tử, trang mạng xã hội phải tuân thủ hướng dẫn bảo mật của nhà cung cấp như quy định về thiết lập mật khẩu gồm chữ thường, chữ in, số, ký tự đặc biệt, độ dài mật khẩu, định kỳ thay đổi mật khẩu, giới hạn số lần nhập sai mật khẩu, không để tên đăng nhập và mật khẩu mặc định, dễ đoán; bật tính năng cảnh báo đăng nhập trên thiết bị lạ (nếu có), không sử dụng một mật khẩu cho nhiều ứng dụng, dịch vụ, trang web; cập nhật đầy đủ phiên bản mới của ứng dụng.

3. Cài đặt và sử dụng các phần mềm diệt virus có bản quyền, thường xuyên rà quét virus, mã độc; tuyệt đối không kích vào đường dẫn lạ, tin nhắn kèm đường dẫn lạ, đọc thư điện tử từ địa chỉ lạ; không lưu thông tin đăng nhập của tài khoản vào trình duyệt web, khi không sử dụng phải đăng xuất khỏi tài khoản; không tải phần mềm từ các website không chính thống, website trung gian, các file từ người lạ gửi qua tin nhắn hoặc thư điện tử lạ.

4. Sử dụng giao thức HTTPS cho website, thiết lập cơ chế xác thực 2 bước. Với các trang/cổng thông tin của cơ quan nhà nước đăng ký tên miền **.gov.vn** theo quy định của Bộ Thông tin và Truyền thông nên đề nghị đánh giá và chứng nhận tín nhiệm mạng nhằm tăng cường mức độ uy tín của các website đối với người dân và để hỗ trợ ngăn chặn việc lợi dụng tên miền thực hiện các hành vi lừa đảo. Đối với các trang Facebook (fanpage) nên tạo lập riêng 02 tài khoản facebook cá nhân chính danh để nắm quyền quản trị viên, tài khoản này phục vụ nắm quyền

quản trị page, và dự phòng, không sử dụng các tài khoản này vào mục đích khác. Các tài khoản khác chỉ được phân quyền biên tập, không phân quyền thêm hoặc xóa thành viên.

5. Thường xuyên tuyên truyền nâng cao ý thức cảnh giác trong công tác bảo mật, bảo đảm an toàn, an ninh mạng, đăng tải, chia sẻ, cung cấp thông tin trong quá trình sử dụng mạng xã hội đối với cán bộ công chức, viên chức, người lao động trong cơ quan.

6. Phân công cán bộ có trình độ chuyên môn, phẩm chất chính trị quản trị trang thông tin điện tử, trang mạng xã hội của đơn vị.

Trong quá trình triển khai thực hiện có khó khăn, vướng mắc đề nghị các đơn vị trao đổi về Công an thành phố Hải Phòng (qua đồng chí Phạm Văn Định – Đội trưởng Đội 2, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, điện thoại 0979.999.356) để phối hợp thực hiện./.

Nơi nhận:
- Như trên;
- Công an Thành phố (để b/c);
- Sở Thông tin và Truyền thông (để b/c);
- TT Huyện ủy;
- CT, PCT Uông Minh Long;
- Lưu: VT.

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

Uông Minh Long