

Số: /UBND-VHTT
V/v khẩn trương rà soát, khắc
phục trang thông tin điện tử
đang bị lợi dụng chèn nội dung
quảng cáo không phù hợp.

Thọ Xuân, ngày tháng năm 2024

Kính gửi:

- UBMTTQ; Các tổ chức đoàn thể chính trị cấp huyện;
- Các phòng, ngành, cơ quan, đơn vị cấp huyện;
- Chủ tịch UBND các xã, thị trấn.

Thực hiện Công văn số 1476/STTTT-CNTT&TT ngày 24/6/2024 của Sở Thông tin và Truyền thông về việc rà soát, khắc phục trang thông tin điện tử đang bị lợi dụng chèn nội dung quảng cáo không phù hợp.

Trong thời gian qua một số trang thông tin điện tử thuộc quản lý của một số cơ quan, đơn vị (có tên miền .gov.vn) bị chèn các liên kết chứa nội dung quảng cáo, kèm theo đường dẫn tới các website cá độ, đánh bạc trực tuyến, mại dâm; khi bấm vào link thì lại chuyển hướng truy cập đến website của tổ chức cá độ, cờ bạc trực tuyến, website khiêu dâm. Chủ tịch UBND huyện yêu cầu các cơ quan, đơn vị, Chủ tịch UBND các xã, thị trấn thực hiện các nội dung sau:

1. Tổ chức rà soát ngay các bài viết có nội dung quảng cáo liên quan cá độ bóng đá, đánh bạc trực tuyến và các nội dung trái quy định của pháp luật trên trang thông tin điện tử của cơ quan, đơn vị trực thuộc, UBND cấp xã để kịp thời gỡ bỏ (có phụ lục hướng dẫn kèm theo).

2. Tăng cường các biện pháp bảo đảm an toàn thông tin mạng, chủ động rà soát, khắc phục điểm yếu, lỗ hổng bảo mật còn tồn tại (nếu có); bổ sung tính năng lưu trữ địa chỉ IP của người dùng, mã CAPTCHAR khi người dùng truy cập, đăng tải nội dung lên trang thông tin điện tử nhằm phục vụ kiểm soát trong trường hợp cần thiết.

3. Rà soát và bổ sung trong quy chế quản lý, vận hành trang thông tin điện tử, trong đó, quy định rõ việc kiểm tra, kiểm duyệt nội dung người dùng đăng tải trước khi cho phép hiển thị lên trang thông tin điện tử. Quản trị viên của trang thông tin điện tử không thực hiện kiểm soát tốt tài khoản quản trị, dẫn đến lộ/loạt thông tin tài khoản.

Trong quá trình thực hiện, nếu có vướng mắc cần hỗ trợ, đề nghị các cơ quan, đơn vị phối hợp với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (thuộc Sở Thông tin và Truyền thông) để được hướng dẫn thực hiện. Đầu mối liên hệ: Ông Trần Ngọc Hưng - Phó Giám đốc Trung tâm CNTT&TT

Thanh Hóa, điện thoại: 0916.422.583. Hoặc bà Nguyễn Huyền Trang, Chuyên viên CNTT, VNPT Thọ Xuân - Thường xuân, điện thoại 0947888765.

Nơi nhận:

- Như trên;
- Chủ tịch, các PCT UBND huyện;
- Lưu VT, VHTT.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Nguyễn Xuân Hải

PHỤ LỤC: Hướng dẫn rà soát, gỡ bỏ nội dung không phù hợp

1. Vị trí thường bị chèn các nội dung quảng cáo không phù hợp

- Mục hỏi đáp, góp ý, bình luận trên các trang thông tin điện tử.
- Tin tặc tấn công trang thông tin điện tử và tải lên mã độc, tập tin quảng cáo nội dung không phù hợp.

2. Rà soát, gỡ bỏ nội dung quảng cáo bất hợp pháp trên Cổng/trang thông tin điện tử do đơn vị quản lý.

- Sử dụng các công cụ tìm kiếm Google, Bing, Yahoo... để tìm kiếm các bài viết có nội dung quảng cáo bất hợp pháp trên Cổng/trang thông tin điện tử.

Ví dụ: Cú pháp trên công cụ tìm kiếm Google:

Site: "tenmien.gov.vn" + "tukhoa"

Trong đó:

+ tenmien.gov.vn là tên miền Cổng/trang thông tin điện tử do đơn vị quản trị, vận hành cần rà soát

+ tukhoa: là từ khóa, tên miền quảng cáo bất hợp pháp cần tìm kiếm trên Cổng/trang thông tin điện tử. Ví dụ: "dk8", "nhà cái", "dk8.com"...

3. Rà soát cơ sở dữ liệu, mã nguồn, máy chủ trang thông tin điện tử

- Quản trị viên đăng nhập hệ quản trị cơ sở dữ liệu, thực hiện truy vấn tìm kiếm các từ khóa quảng cáo bất hợp pháp từ các bảng (hỏi đáp, bình luận, góp ý...) lưu trữ thông tin mà người dùng gửi lên.

Ví dụ: `select * from tbl_hoidap where noidungcauhoi like "%từ khóa%"`

- Rà soát mã độc, webshell mà tin tặc đã tải lên hệ thống. Có thể sử dụng các công cụ như: Shell detector tại địa chỉ shelldetector.com; các công cụ so sánh, phát hiện sự thay đổi của các tệp tin mã nguồn Cổng/trang thông tin điện tử so với mã nguồn gốc; sử dụng các công cụ phòng chống mã độc...

4. Tăng cường bảo đảm an toàn thông tin cho các trang thông tin điện tử

4.1. Đối với các Cổng/trang thông tin điện tử đã bị tấn công:

- Thêm header hoặc thẻ no-index cho các đường dẫn uploads để thông báo cho công cụ tìm kiếm biết rằng không index các đường dẫn, tệp mà người dùng gửi lên.

- Gỡ bỏ các tệp pdf có chứa nội dung backlink.

- Xác định lỗ hổng XSS hoặc phần tìm kiếm, khắc phục các lỗ hổng này lại.

- Xác định các lỗ hổng RCE, Upload file, SQL Injection, các CVE nếu có và khắc phục lại các lỗ hổng này.

- Sử dụng HTTP method POST cho các form tìm kiếm thay vì GET.
- Thông báo, yêu cầu các công cụ tìm kiếm (Google, Bing...) gỡ bỏ bài viết đã được index.

4.2. Đối với Công/trang thông tin điện tử chưa bị tấn công:

- Rà soát định kỳ và đánh giá tổng thể an toàn bảo mật cho Công/trang thông tin điện tử để tìm kiếm các lỗ hổng, điểm yếu và khắc phục kịp thời.
- Thêm header hoặc thẻ no-index cho các đường dẫn uploads để thông báo cho công cụ tìm kiếm biết rằng không index các đường dẫn, tệp mà người dùng gửi lên.
- Rà soát lỗ hổng XSS, File upload, SQL Injection, các CVE và chức năng tìm kiếm của website.
- Sử dụng HTTP method POST cho các form tìm kiếm thay vì GET.
- Bổ sung mã CAPTCHAR tại các mục cho phép người dùng có thể đăng tải nội dung (Mục hỏi đáp, góp ý, bình luận) lên Công/trang thông tin điện tử để ngăn chặn các công cụ tự động đăng tải.
- Kiểm duyệt các nội dung người dùng đăng tải trước khi cho phép hiển thị lên Công/trang thông tin điện tử.