

PHỤ LỤC

Hướng dẫn rà soát, gỡ bỏ quảng cáo độc hại trên Trang/Cổng TTĐT
(Kèm theo Công văn số /UBND-VP6 ngày /02/2024 của UBND tỉnh)

I. HƯỚNG DẪN RÀ SOÁT CÁC NỘI DUNG QUẢNG CÁO ĐỘC HẠI TRÊN TRANG TTĐT DO ĐƠN VỊ QUẢN LÝ

1. 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 Trang TTĐT:

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

site: "tenmien.gov.vn" intext:"từ khóa"

Trong đó:

- **tenmien.gov.vn** là tên miền Trang TTĐT do đơn vị quản trị, vận hành cần rà soát.

- **từ khóa**: là từ khóa, tên miền quảng cáo bất hợp pháp cần tìm kiếm trên Trang TTĐT. Ví dụ: "dk8", "nhà cái", "dk8.com", "88.com", "tài xỉu", "nổ hũ", "game", "fun88", "lô đề", "bắn cá"...

2. 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%"**

3. Rà soát mã độc, webshell mà tin tặc đã tải lên hệ thống. Có thể sử dụng các công cụ Shell Detector tại đại chỉ shelldetector.com; các công cụ so sánh, phát hiện sự thay đổi của các tập tin mã nguồn trang TTĐT so với mã nguồn gốc; sử dụng các công cụ antivirus...

II. HƯỚNG DẪN KHẮC PHỤC, NGĂN CHẶN CÁC TRANG WEB BỊ CHÈN QUẢNG CÁO ĐỘC HẠI

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

2. Rà soát máy chủ, gỡ bỏ các tệp pdf, text, html được tải lên máy chủ có chứa nội dung quảng cáo độc hại.

3. Sử dụng HTTP method POST cho các form tìm kiếm thay vì GET. Bổ sung mã CAPTCHA tại các mục cho phép người dùng có thể đăng tải nội dung (Mục hỏi đáp, góp ý, bình luận...) trên Trang TTĐT để ngăn chặn các công cụ tự động đăng tải.

4. Rà soát các lỗ hổng bảo mật như XSS, SQL Injection, RCE, Upload file và vá các lỗ hổng này trên Trang thông tin điện tử.

5. Thông báo, yêu cầu Google gỡ bỏ bài viết đã được index./.