CÔNG TY CỔ PHẦN **ĐẠI LÝ HÀNG HẢI VIỆT NAM**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 239/CV-VOSA/TGĐ V/v *Cảnh báo lừa đảo qua Website và phòng tránh rủi ro*	*TP. Hồ Chí Minh, ngày 02 tháng 07 năm 2024*

Kính gửi: - CÁC CÔNG TY TNHH
- CÁC CHI NHÁNH TRỰC THUỘC
- CÁC PHÒNG CMNV CÔNG TY

Trước tình trạng lừa đảo xuất hiện trên Website ngày càng phức tạp và nhiều gây hậu quả nặng nề về tinh thần lẫn tài chính của nhiều người. Thời gian vừa qua VOSA cũng đã có trường hợp làm giả mạo trang Website của VOSA để lừa đảo tuyển dụng như: https://vosa-vn.com hay htpps://vosa-"bất cứ tên nào"… và email tuyendung@vosa-com.vn … mà người dùng rất dễ bị nhầm lẫn giống trang Website của VOSA đang sử dụng **https://vosa.com.vn** hay **https://vosa.vn**, tất cả những trang Website của VOSA đều đã được đăng ký với Trung tâm quản lý tên miền Việt Nam. Đây là hình thức lừa đảo qua Website có chủ đích thay đổi nội dung và địa chỉ Email của người gửi, nếu người nhận không kiểm tra đúng Website và Email có thể sẽ gây ra hậu quả rất nghiêm trọng.

Bộ phận IT VOSA tiếp tục đưa ra một số khuyến cáo và biện pháp phòng chống để hạn chế tối đa việc bị lừa đảo qua Website như sau:

1. Cách nhận biết trang Web lừa đảo nhanh qua đường dẫn link độc hại:

Đầu tiên, hãy kiểm tra lại địa chỉ Web. Đây là phương pháp nhanh chóng nhất trong các cách nhận biết trang Web lừa đảo. Cảnh giác trước các đường dẫn có dấu hiệu sau đây:

- Lỗi chính tả: Sai khác, thiếu hoặc thừa một vài ký tự, hoặc thay thế một vài ký tự với ký tự khác gần giống (như "l" thay bằng "1"). Ví dụ: shopeepv.com, fptshopvn.com

- Tên miền sử dụng ký tự lạ. Ví dụ: https://suamaylanh.dien-may-xanh.net.

- Tên miền phụ cố bắt chước tên miền của một trang hợp pháp. Ví dụ: https://shopee.sukientriankhachhang2021.com/, trong đó shopee là tên miền phụ, tên miền thực tế là sukientriankhachhang2021.com.

- Các đuôi trang .com, .org, .gov (chính phủ), .edu (giáo dục đào tạo)… thường là những top-level domain có thể tin cậy được, tuy nhiên cũng cần phải cẩn trọng khi truy cập nếu bạn thấy có dấu hiệu khả nghi về việc lấy cắp hay thu thập thông tin dữ liệu cá nhân. Vì vậy nên xác nhận lại mọi thứ. Trong khi đó, các đuôi top-level domain ít phổ biến như .info, .asia, .vip, .tk, .xyz… thường có độ tin cậy khá là thấp. Tên miền có top-level domain có độ tin cậy thấp. Ví dụ: https://www.shoppe8.vip, top-level domain là .vip hoặc https://vngame.xyz.

• Đường dẫn sử dụng tên miền quốc tế (IDN) fàcebook.com – chữ "à" là một ký tự đặc biệt (domain thật: xn--fcebook-8va.com) để đánh lừa nạn nhân.

• Sử dụng dịch vụ rút gọn tên miền dạng như bitly.com, cutt.ly, shorturl.at – những kiểu lừa đảo dựa trên những link phishing dạng này nên cẩn trọng và không click vào, nếu tò mò có thể sử dụng: browserling.com hay urlscan.io để check xem link ấy thế nào.

2. Cách nhận biết trang Web lừa đảo qua giao diện trang Web:

Xem kỹ giao diện Web. Cách nhận biết Web lừa đảo này rất dễ nhận biết vì Website thật thường giao diện rất chuyên nghiệp, tương thích cho cả điện thoại, laptop hay máy tính bảng, hãy để ý các yếu tố như logo, hình nền và chắc chắn rằng chúng không phải là phiên bản nhái (sai khác về chi tiết, màu sắc) hay phiên bản lỗi thời (sử dụng hình ảnh phiên bản cũ). Một trang Web sử dụng hình ảnh không đúng quy chuẩn thương hiệu chắc chắn là trang Web không an toàn.

3. Cách nhận biết trang Web lừa đảo dựa vào nội dung trên Web:

Các bạn hãy chú ý đến nội dung Web. Các trang Web lừa đảo không an toàn sẽ để lộ những điểm yếu sau:

• Thông tin đơn vị chủ quản Website không chính xác. Ví dụ, Website giả mạo có thể sử dụng đúng tên doanh nghiệp nhưng cung cấp số tổng đài hoặc địa chỉ không có thực. Ở Việt Nam các bạn có thể tra thông tin công ty tại: tratencongty.com và nếu bạn thấy biểu tượng của Bộ Công Thương trên trang Web mà bạn lo lắng, hãy thử nhấp vào biểu tượng đó! Nếu bạn thấy rằng chức năng này không hoạt động, hãy truy cập "Hệ thống quản lý thương mại điện tử" thuộc "Bộ Công Thương" tại online.gov.vn và kiểm tra xem họ có phải là người dùng con dấu tin cậy được chứng nhận hay không.

• Nội dung chứa lỗi chính tả. Nguyên nhân là do các trang Web giả mạo thường không kiểm duyệt kỹ nội dung. Hoặc, các trang này được tạo bởi kẻ xấu ở nước ngoài mà họ không thành thạo ngôn ngữ được sử dụng để lừa đảo.

• Chú ý các liên kết đến các trang mạng xã hội của một trang Web. Các nút liên kết mạng xã hội có thể dẫn đến trang chủ của trang Web.

4. Cách nhận biết trang Web lừa đảo qua những thông báo trên Web:

Cảnh giác với các thông báo có nội dung "giật gân" trên Web. Trang Web giả mạo thường sẽ "nhử" mọi người bằng cách đưa ra những thông báo khiến mọi người quá hoảng sợ, hoặc quá vui mừng. Ví dụ như thông báo về sự cố giao dịch hoặc thông báo trúng thưởng, khuyến mãi, quà tặng…. kèm theo đó là yêu cầu mọi người nhập thông tin tài khoản, mật khẩu, số thẻ tín dụng để xác minh. Một trang Web thật sự sẽ không có tin như trên. Ngoài ra, mọi người cũng nên cẩn thận trước các lời mời tải phần mềm trên các trang Web lạ, đặc biệt là những trường hợp sau:

• Lời mời tải xuống phần mềm kèm theo thông báo thiết bị đã bị nhiễm virus.

• Lời mời tải miễn phí nội dung có bản quyền đắt tiền.

• Lời mời tải xuống "siêu phần mềm" (như tăng tốc độ máy tính, bẻ khóa Wi-Fi, hack facebook, gmail, tài khoản game…).

• Lời mời xem những nội dung nhạy cảm, hay đánh vào lòng tốt và tin giật gân gây shock.

• Lời mời tham gia kiếm tiền nhanh, giới thiệu mọi người bạn bè để nhận hoa hồng cao.

5. Những vấn đề đáng quan tâm khác mà gần đây đang có dấu hiệu gia tăng:

Chạy quảng cáo bẩn trên các nền tảng mạng xã hội, hay Google để quảng bá về trang lừa đảo của bọn chúng. Và đồng thời làm những video quảng cáo trên Youtube để dẫn dụ nạn nhân. Các dạng này đều có chung hình thức bắt trả phí online hoặc cung cấp mật khẩu tài khoản. Lợi dụng lòng tham, tâm lý sợ hãi… mà những trang này làm nạn nhân mất luôn cả tài khoản Facebook, Email, tài khoản game, ngân hàng và lừa đảo thẻ cào điện thoại.

6. Liên hệ ngay với bộ phận IT Công ty nếu phát hiện có bất thường trong khi sử dụng máy tính: phát hiện sớm các rủi ro để ngăn chặn.

Đề nghị các Chi nhánh/Công ty TNHH và các phòng CMNV Công ty nghiêm túc thực hiện và triển khai thông tin đến toàn thể CBNV đơn vị mình những khuyến cáo về Cảnh báo lừa đảo qua trang Website nêu trên để có thể tự bảo vệ và phòng tránh những rủi ro an toàn trước môi trường số hóa ngày càng phức tạp.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc vui lòng liên hệ Tổ IT VOSA qua địa chỉ E-mail: hungnp.vsa@vosagroup.com để được hỗ trợ, hướng dẫn.

Trân trọng kính chào.

Nơi nhận:
- Như trên;
- PTGĐ PT, các PTGĐ;
- Lưu: VT, P. THPC, NPH.

TL. PHÓ TỔNG GIÁM ĐỐC PHỤ TRÁCH
TRƯỞNG PHÒNG THPC

M.S.D.N: 0300437898 - C.T.C.P
CÔNG TY CỔ PHẦN ĐẠI LÝ HÀNG HẢI VIỆT NAM
QUẬN 7 - T.P HỒ CHÍ MINH

Trần Công Toàn