

Số: 29/CATTT-TTTV

Hà Nội, ngày 24 tháng 01 năm 2018

V/v cảnh báo chiến dịch tấn công lừa đảo thông qua các chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính.

Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông tin đã phát hiện đang có nhiều chiến dịch tấn công lừa đảo nhắm vào người sử dụng Internet Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Những chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, các ngân hàng, các cơ sở dịch vụ lớn, các chương trình trúng thưởng để thu thập thông tin cá nhân người sử dụng, các tài khoản mạng xã hội, các tài khoản ngân hàng, thẻ tín dụng .v.v...

Các đối tượng tấn công lợi dụng thời điểm cuối năm, cận tết Âm Lịch có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng đồng thời tâm lý và thói quen mua sắm vội vàng cuối năm làm cho nhiều người dùng mất cảnh giác.

Cục An toàn thông tin đã phát hiện có ít nhất 700 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên (*thông tin chi tiết về chiến dịch tấn công và một số tên miền phishing xin tham khảo tại Phụ lục kèm theo*).

Nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công lừa đảo, Cục An toàn thông tin khuyến nghị:

- Người dùng cần cảnh giác với những tin nhắn với các thông tin khuyến mãi, trúng thưởng, nhận thưởng. Không click vào bất cứ liên kết lạ nào được nhận từ tin nhắn trên facebook, kể cả từ các tài khoản bạn bè và người thân và các kênh tương tự như Zalo, Viber;

- Cảnh giác với những địa chỉ web lạ, gọi mở về việc nhận thưởng, trao giải. Trong trường hợp cần thiết, xin vui lòng liên hệ với chủ quản của nhãn hiệu đó để xác minh;

- Cập nhật mật khẩu tài khoản facebook, sử dụng các mật khẩu mạnh, chưa từng được sử dụng trước đó, bật tính năng xác thực 2 bước do facebook cung cấp;

- Không cung cấp tài khoản mạng xã hội, tài khoản ngân hàng, thông tin cá nhân hay các thông tin riêng khác trên bất kỳ trang web không chính thống nào;

- Trong trường hợp cần thiết, xin vui lòng liên hệ Cục An toàn thông tin, số điện thoại: 024.3943.6684, thư điện tử ais@mic.gov.vn hoặc fanpage Trung tâm xử lý tấn công mạng Internet Việt Nam theo đường dẫn <https://www.facebook.com/govSOC/> để được hỗ trợ kịp thời.

Trân trọng./.

Nơi nhận:

- Như trên;
- Lãnh đạo Bộ (đề b/c);
- Cục trưởng (đề b/c);
- Lưu: VT, TTTV.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Nguyễn Huy Dũng

Phụ lục

Chiến dịch tấn công lừa đảo thông qua các chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng (Kèm theo Công văn số 29/CATTT-TTTV ngày 24/01/2018)

Qua công tác giám sát và theo dõi tình hình, Cục An toàn thông phát hiện đang có nhiều chiến dịch tấn công lừa đảo nhắm vào người sử dụng mạng Internet tại Việt Nam, đặc biệt là những người dùng mạng xã hội Facebook. Các chiến dịch lừa đảo này tạo ra hàng loạt trang web giả mạo các mạng xã hội, ngân hàng, nhà cung cấp dịch vụ lớn, các chương trình trúng thưởng để thu thập thông tin cá nhân, tài khoản mạng xã hội, tài khoản ngân hàng, thẻ tín dụng .v.v... của người sử dụng.



SỰ KIỆN TRI ÂN KHÁCH HÀNG NHÂN DỊP ĐÓN NĂM MỚI 2018

XIN CHÚC MỪNG LƯỢT QUAY CỦA BẠN ĐÃ MAY MẮN TRÚNG GIẢI NHẤT

CHƯƠNG TRÌNH QUAY SỐ NGẪU NHIÊN
Khách hàng trúng giải nhất với mã số code là
TN5279

PHÂN QUẢ QUÝ KHÁCH MAY MẮN NHẬN ĐƯỢC GỒM

Mã số trúng thưởng CHÚNG GIẢI NHẤT	Tri ân khách hàng	1 Xe Honda SH 150i
200.000.000 VND		1 Phiếu Quà Tặng Trị Giá 200.000.000 VND
		1 Phiếu Đổ Xăng Miễn Phí Của Petrolimex Trị Giá 5.000.000 VND

Một số hình ảnh sử dụng trong chiến dịch tấn công phishing

Các đối tượng tấn công lợi dụng thời điểm cuối năm, thời gian cận tết Âm lịch có nhiều chương trình khuyến mại, giảm giá, tặng quà tri ân cho khách hàng; đồng thời tâm lý và thói quen mua sắm vội vàng cuối năm làm cho nhiều người dùng mất cảnh giác.

THÔNG TIN CỦA QUÝ KHÁCH

Vui lòng cập nhật thông tin đầy đủ để nhận thưởng !

Họ và Tên 🔒

Ngày Tháng Năm Sinh

Tỉnh/Thành Phố

Địa Chỉ Cư Trú: Số Nhà (nếu có), Thôn (Xóm,Ấp), Xã (Phường), Ht

Giới Tính (Nam/Nữ)

Số Chứng Minh Nhân Dân

Số Điện Thoại Liên Hệ

Nghề Nghiệp

Màu Xe (Trắng / Đen / Đỏ / Xanh)

Email hoặc Số Điện Thoại FaceBook

Mật Khẩu FaceBook 🔒

Thẻ ATM (Nếu không có thì vui lòng bỏ trống)

Tên Chủ Thẻ

Tên Ngân Hàng + Chi Nhánh

Số Tài Khoản

**Sau khi điền đầy đủ Thông Tin
Vui lòng bấm vào nút " CẬP NHẬT HỒ SƠ " bên dưới.**

CẬP NHẬT HỒ SƠ

Vui Lòng Cập Nhật Thông Tin Đầy Đủ Để Nhận Thưởng!

Thông Tin Không Có Vui Lòng Điền "Không Có"!

Vui Lòng Nhập Chính Xác Thông Tin Cá Nhân Để Hồ Sơ Hợp Lệ!

Họ và Tên 🔒

Ngày Sinh

Bưu Điện Tỉnh/Thành Phố

Địa Chỉ Cư Trú

Giới Tính

Số Chứng Minh Nhân Dân

Số Tài Khoản Ngân Hàng

Tên Chủ Thẻ + Chi Nhánh

Điện thoại

Nghề Nghiệp

Màu Xe (Trắng,Đen,Đỏ)

SDT hoặc Email FaceBook

Mật Khẩu 🔒

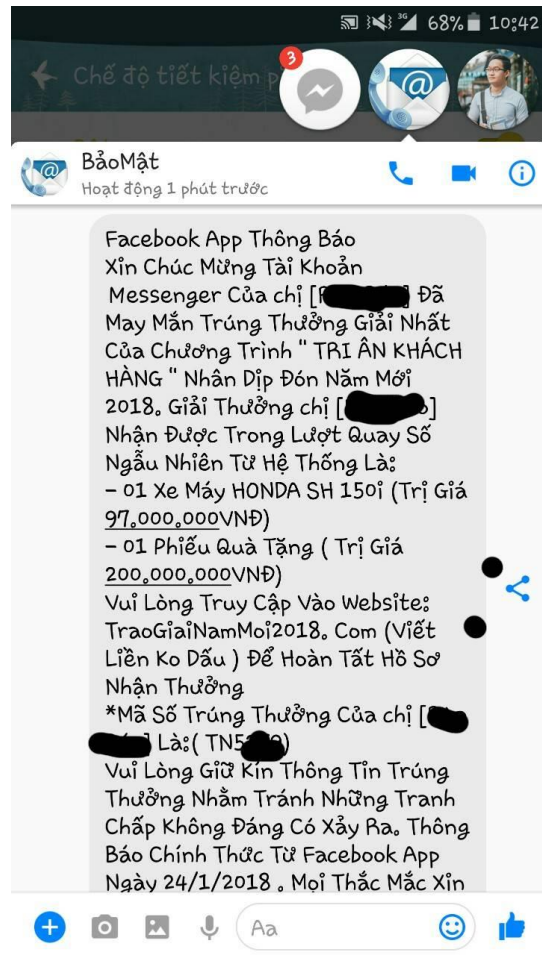
Mã Số Trúng Giải

Vui Lòng Điền Đầy Đủ Thông Tin, Thông Tin Không Có Vui Lòng Điền : "Không Có"

Cập nhật hồ sơ dự thưởng

Các trang web lừa đảo yêu cầu người dùng nhập thông tin cá nhân, thẻ ATM và mật khẩu Facebook

Các trang web lừa đảo được đối tượng tấn công lan truyền và quảng bá đến người dùng thông qua nhiều kênh khác nhau, trong đó kênh được sử dụng nhiều nhất hiện tại là Facebook Messenger. Để gia tăng sự tin tưởng của người dùng, các thông tin lừa đảo khi lan truyền còn được kèm theo các đoạn mã được quảng cáo là mã trúng thưởng.



Tấn công phishing lan truyền qua Facebook Messenger.

Cục An toàn thông tin đã phát hiện có ít nhất 700 tên miền được sử dụng để phục vụ cho các chiến dịch tấn công lừa đảo nói trên. Hầu hết các trang web đều sử dụng tên miền được đăng ký gọi mở đến chương trình trúng thưởng, trao giải như:

- hosofacebook.com
- hosofb68669.com
- hopqua2018.com
- nhanquatet2018.com
- nhanthuong2018.com
- traogiainammoi2018.com
- quacuoinam2018.com
- mochathuongtet2018.com

(Số lượng các trang web lừa đảo rất lớn sẽ được Cục ATTT cập nhật thường xuyên tại <https://khonggianmang.vn/warn/phishing.txt>)