

Vụ 31.000 thông tin cá nhân bị lộ, liệu khách có mất tiền?

08:58 09/11/2018

Ngày 7-11, thông tin của hơn 31.000 giao dịch thẻ ngân hàng (NH) và hơn 5 triệu email được cho là của khách hàng Thế Giới Di Động (TGDĐ) bị tài khoản erchowin chia sẻ trên Internet. Đến hôm qua (8-11), tin tức tiếp tục đẩy các thông tin liệt kê đầy đủ 16 chữ số thẻ tín dụng của những tài khoản được cho là của khách hàng TGDĐ.

Thực hư chuyện Thế Giới Di Động “hack”...?

Liên quan đến nguồn thông tin lan truyền trên mạng cho rằng hệ thống công nghệ của Công ty cổ phần Thế Giới Di Động (gọi tắt là TGDĐ) “bị hacker tấn công và lấy cắp thông tin cá nhân khách hàng”, phía doanh nghiệp bán lẻ thiết bị điện tử này cũng đã phát ra thông cáo báo chí cho biết đó là thông tin không chính xác.

Các chuyên gia bảo mật khi được hỏi cũng chưa dám xác nhận do các dữ liệu được công bố không được kiểm chứng rõ ràng. Song, vụ việc này một lần nữa cảnh báo về việc bảo vệ thông tin cá nhân (TTCN) hiện đang bị thả lỏng.



*Quá dễ dàng tìm thấy thông tin được cho là của khách hàng Thế Giới Di Động
rao trên diễn đàn RaidForums (Ảnh IT)*

Có thể tóm tắt diễn biến vụ việc khách hàng TGDĐ nghi bị đánh cắp TTCN như sau: Từ sáng 7-11, đã có thông tin đăng tải trên diễn đàn RaidForums về việc có trong tay thông tin hơn 5 triệu khách hàng của TGDĐ. Các thông tin từ đó cũng cho thấy hơn 31.000 bản ghi lịch sử giao dịch của khách hàng với TGDĐ và Điện máy Xanh. Cùng với đó có khoảng 5,4 triệu email khách hàng và thậm chí có 61.000 email hệ thống mail nội bộ của TGDĐ.

Các thông tin về lộ thông tin của khách hàng còn tiếp diễn sau đó, một tập tin đầy đủ được cho là đánh cắp từ TGDĐ cho thấy lịch sử giao dịch của năm 2016 với số hiệu đơn vị, địa chỉ mua hàng, số thẻ tín dụng... của khách hàng. Ngay tối cùng ngày, TGDĐ đã phát thông cáo báo chí, cho rằng nguồn tin lan truyền trên mạng nói trên là thông tin không chính xác.

Trước sự việc này, ông Nguyễn Hữu Cường (chuyên gia bảo mật của Bkav, người điều hành Diễn đàn An ninh mạng whitehat.vn) cho biết: Hiện giờ chưa có bằng chứng khẳng định đây là thông tin khách hàng của TGDĐ. Cùng với đó, nếu giả sử đây đúng là khách hàng của TGDĐ thì cũng chưa thể xác định việc lộ lọt thông tin ở đâu, thuộc trách nhiệm của ai. Tuy nhiên Bkav khuyến cáo người dùng nên chủ động kiểm tra xem địa chỉ email và tài khoản của mình có nằm trong các tập tin đã đăng tải trên RaidForums để đảm bảo an toàn.

Ông Ngô Tấn Vũ Khanh, Giám đốc Phát triển Kaspersky Lab Việt Nam, cũng nhận định: Việc hệ thống đơn vị này có bị hack và lộ thông tin khách hàng hay không cần phải điều tra thực tế và có đánh giá của các chuyên gia. Nhưng đây rõ ràng là hồi chuông cảnh báo cho các công ty lớn, có một hệ thống công nghệ thông tin đồ sộ, cần phải quan tâm đến hơn nữa vấn đề bảo mật. Trong trường hợp này, việc cài đặt phần mềm bảo mật vào các máy POS là rất quan trọng vì hacker có thể chiếm quyền điều khiển máy POS và làm bàn đạp tấn công các giao dịch nếu thiết lập được một giao thức đủ tốt. Tuy nhiên thực tế hiện nay tỷ lệ các công ty bán lẻ tại Việt Nam quan tâm đến bảo mật trên các máy POS là rất thấp (chưa tới 5%).

Trước sự kiện trên, nhiều người lo lắng thông tin thẻ sẽ bị kẻ xấu lợi dụng, đánh cắp tiền. Anh T. (nhà ở quận Tân Bình, TP.HCM) chia sẻ: “Tôi thường mua hàng ở TGDĐ. Khi thanh toán mua hàng tôi cũng hay cà thẻ ATM. Vậy không biết thẻ của tôi có bị hacker tấn công không, có nguy hiểm gì không? Bên cạnh đó, khi đi mua hàng trả góp, tôi phải cung cấp các thông tin liên quan như số điện thoại, email, địa chỉ... cho doanh nghiệp. Điều này khiến tôi cảm thấy bất an”.

Đặc biệt, nhiều người dùng xác nhận họ chưa từng mua sắm tại TGDĐ nhưng email vẫn nằm trong danh sách rò rỉ. Do đó, rất có thể hacker đã thu thập email từ nhiều nguồn khác nhau, bởi trong danh sách này có rất nhiều email mang tên miền công ty như Asus, Acer, Bkav...

Khách hàng lo lắng, ngân hàng trấn an

Trao đổi với báo chí, một số lãnh đạo NH cho rằng kể cả hacker có đủ 16 chữ số trên thẻ cũng chưa thể lấy được tiền của người gửi tiền. Chỉ trong trường hợp bị lộ tất cả thông tin về số thẻ, ngày hết hạn, ba số bí mật phía sau thẻ (mã CVV)... đối tượng xấu mới có thể thực hiện giao dịch trên mạng.



Khách lo lắng bị kẻ xấu lợi dụng thông tin rò rỉ để đánh cắp tiền, trong khi Thế Giới Di Động cho rằng mình không để lộ thông tin (Ảnh: HTD)

Phó tổng giám đốc một NH giải thích thêm: Mã CVV là dữ liệu mà chỉ có NH biết chứ một bên là điểm chấp nhận thanh toán (merchant) như TGDĐ không thể có được. Vì vậy, nếu dữ liệu này được tin tặc lấy từ đây như họ tuyên bố thì cũng không thể có số CVV.

Mặt khác, những thông tin mà tin tặc có trong tay chưa đủ để lấy tiền từ tài khoản của người dùng. Tuy vậy, vị lãnh đạo NH này cho biết sẽ chờ đánh giá của cơ quan chức năng để đi đến quyết định có thay lại toàn bộ thẻ tín dụng cho khách của mình hay không.

Tính đến thời điểm hiện tại, chưa có thông tin về những rủi ro nguy hiểm cho chủ thẻ do bị lộ thông tin. Nhưng đại diện một số NH cho hay đã cho rà soát lại toàn bộ dữ liệu cũng như phân tích các yếu tố liên quan để xác định xem có rủi ro hay không. Trong trường hợp có nguy cơ rủi ro sẽ cảnh báo ngay cho khách hàng.

Ông Lê Minh Huấn, Phó Tổng Giám đốc NH Thương mại Cổ phần Sài Gòn (SCB), cho biết: Mặc dù phía TGDĐ đã xác nhận là hệ thống thông tin của họ vẫn an toàn nhưng để an toàn cho ví tiền của mình và để tránh rủi ro có thể xảy ra, tốt

nhất những khách hàng nào từng thực hiện giao dịch bằng thẻ tại TGDĐ nên đến NH để đổi thẻ mới ngay.

“Về phía SCB, bên cạnh việc chờ đợi xác minh lại một lần nữa từ phía các cơ quan chức năng để xác định xem dữ liệu bị rò rỉ có phải xuất phát từ TGDĐ hay không, chúng tôi liên tục quan sát các giao dịch bất thường trên hệ thống nhờ hệ thống công nghệ thông tin và quan sát của con người. Nếu khi thấy có giao dịch bất thường, chúng tôi sẽ gọi điện thoại ngay cho khách hàng để xác minh giao dịch” - phó tổng giám đốc NH SCB cho biết.

Một số chuyên gia về NH cũng khuyến cáo: Để bảo đảm an toàn, tốt nhất người dùng nên đổi mật khẩu email cá nhân; thay đổi mật khẩu giao dịch NH online banking hoặc tạm thời đóng băng giao dịch bằng thẻ tín dụng để chờ xác minh.

Hải Đăng