PHISHER SỬ DỤNG... CỔNG THÔNG TIN CHÍNH PHỦ MALAYSIA ĐỂ LỪA ĐẢO

Một âm

Một âm mưu lừa đảo phishing tinh vi vừa được phát hiện, trong đó, những kẻ chủ mưu đã sử dụng máy tính thuộc Chính phủ Malaysia và một công ty y tế uy tín.

Bill Carton là một kỹ sư đang làm việc tại San Diego nhưng đã có thâm niên 10 làm chuyên gia chống thư rác tình nguyện. Anh đã tình cờ phát hiện thấy âm mưu nói trên khi nhận một bức email mạo nhận là gửi đi từ dịch vụ PayPal của eBay hôm thứ bảy tuần trước.

Nội dung của nó y hệt những email lừa đảo trước đây: "Chúng tôi được biết thông tin tài khoản của bạn cần được cập nhật. Nếu bạn có thể tạm dừng công việc đang làm 5-10 phút và cập nhật các thông tin cá nhân của mình, bạn sẽ không gặp phải bất cứ trục trặc nào trong tương lai với dịch vụ của chúng tôi".

Nguồn: BBC

Tuy nhiên, điểm không bình thường trong vụ lừa đảo này, là đường link bên trong email dẫn tới website PayPal giả lại được lưu ký bởi máy chủ của ... chính phủ Malaysia tại tên miền gov.my. "Dùng tên miền chính phủ thì chịu rồi, ai dám hoài nghi cơ chứ?", Carton bình luận.

Điều tra sâu thêm về bức email, Carton nhận thấy "ngoài máy chủ của chính phủ, kẻ lừa đảo còn sử dụng một nguồn đáng tin cậy khác để gửi đi bức email giả mạo nói trên. Máy chủ mail bị khống chế để phát tán thư rác và xóa sạch dấu vết về spammer không phải là máy tính gia đình thường gặp, mà là của Rxdocuments.com. Họ có lắp đặt hẳn một hệ thống phần mềm bảo vệ riêng tư cá nhân, thế mà lại bị hacker tấn công và lợi dụng để phát tán thư rác".

Rxdocuments.com là website chuyên cung cấp dịch vụ "chép chính tả" cho các dược sĩ. Cả trang web này lẫn chính phủ Malaysia đều chưa đưa ra bình luận nào về phát hiện của Carton.

Theo chuyên gia Paul Laudanski của Computer Corps, đây không phải là lần đầu tiên website gov.my bị giới phisher lợi dụng. Địa chỉ này đã bị sử dụng ít nhất bốn lần kể từ tháng 4 năm nay để gửi đi email giả mạo Citibank, eBay và Chase.

Các âm mưu lừa đảo phishing ngày càng trở nên tinh vi khi bọn tội phạm nhận thấy hoàn toàn có thể kiếm được tiền tươi thóc thật từ hoạt động lừa đảo trực tuyến. Hãng nghiên cứu Gartner ước tính người Mỹ đã thiệt hại tới 2,8 tỷ USD vì nạn phishing trong năm 2006.

"Chưa bao giờ chúng ta chứng kiến hoạt động phishing mạnh và nhan nhản như thế này", ông Dave Jevans, chủ tịch Anti-Phishing Working Group nhận định. "Hai tháng trở lại đây, lượng thư rác tăng đột biến và số lượng các vụ lừa đảo cũng thừa cơ đó leo thang".

Ông Jevans cũng nhất trí rằng vụ mạo danh PayPal mới nhất rất không bình thường. "Thật thú vị khi hai tổ chức mà bạn nghĩ rằng bảo mật nghiêm cẩn lại bị hacker hạ gục và dùng làm vũ khí".

Trọng Cầm