CÁCH NHẬN DẠNG EMAIL LỪA ĐẢO

Theo số liệu thống kê từ hãng bảo mật email MailFrontier, chỉ có... 4% người dùng đủ khả năng nhận dạng email lừa đảo với tỷ lệ chính xác 100%. Đây quả là một thông tin đáng lo ngại khi mùa mua sắm đang đến gần và dân tình bắt đầu đổ xô lên mạn

Theo số liệu thống kê từ hãng bảo mật email MailFrontier, chỉ có... 4% người dùng đủ khả năng nhận dạng email lừa đảo với tỷ lệ chính xác 100%. Đây quả là một thông tin đáng lo ngại khi mùa mua sắm đang đến gần và dân tình bắt đầu đổ xô lên mạng để mua sắm. Kết quả mà MailFrontier đưa ra được căn cứ trên bài kiểm tra Phishing IQ, trong đó liệt kê 10 mẫu email và người sử dụng phải đánh dấu vào những mail nào họ cho là hợp pháp, mail nào là lừa đảo. Các email mẫu đều được lấy từ Chase, PayPal, Ngân hàng trung ương Mỹ, MSN, Earthlink và Amazon. Năm nay, tỷ lệ đúng trung bình của những người tham gia kiểm tra là 75%, tăng so với 61% của năm ngoái. MailFrontier tin rằng sự tiến bộ này là kết quả của việc người sử dụng ngày càng hiểu biết hơn về phishing và biết "nghi ngờ" hơn. Một trong những phát hiện đáng ngạc nhiên của MailFrontier là người dùng trẻ tuổi (18-24) lại dễ bị lừa hơn những người sử dụng lớn tuổi (55+), mặc dù họ sành sỏi về công nghệ mới hơn. 5 điều hoang tưởng về phishing Đóng góp quan trọng nhất của MailFrontier trong kết quả nghiên cứu lần này, là họ đã chỉ ra được 5 điều người ta vẫn hoang tưởng về phishing. 1. "Ồ, phát hiện trò lừa dễ như bóc kẹo ý mà!" Sai lầm lớn nhất của người sử dụng là họ luôn quá tự tin vào khả năng của mình. Mặc dù trình độ nhận biết email phishing của người sử dụng đã có khá nhiều tiến bộ, song điều đó không có nghĩa bất cứ lúc nào họ cũng đủ tỉnh táo và kiến thức để biết rằng mình đang bị lừa. Đa số họ vẫn đánh đồng một email phishing với email hợp pháp. 2. Thế bộ lọc thư rác là đống sắt vụn à? Đại bộ phận người dùng có xu hướng thần thánh hóa các bộ lọc thư rác, cho rằng chúng có thể phát hiện và ngăn chặn mọi cuộc tấn công phishing. Và thế là họ yên tâm, vô tư click vào mọi email xuất hiện trong hòm thư mình. Nên biết rằng để "tóm" được một email lừa đảo cần phải có một loạt công cụ phân tích và đánh giá phức tạp, chứ một mình bộ lọc thư rác thì chỉ biết... "cười trừ" mà thôi. 3. Có thể chặn email phishing bằng xác thực tên miền? Dùng xác thực tên miền như một công cụ để chặn email lừa đảo là điều hoang đường thứ ba. Những kẻ phát tán thư rác, cũng như dân phisher chuyên nghiệp, đã cho thấy chúng hoàn toàn có thể vượt qua cửa ải này. 4. Phát hiển lỗ hổng trong URL chắc cũng phải chặn được email phishing chứ? Lỗ hổng trong địa chỉ URL là một dấu hiệu tốt để nhận biết có điều gì đó không đúng, nhưng bản thân nó lại không thể làm một bằng chứng thuyết phục. Nhiều công ty hợp pháp vẫn sử dụng các kỹ thuật như redirect địa chỉ URL, sử dụng URL dài (vượt quá độ dài của thanh biểu tượng) và kể cả là địa chỉ IP thô trong các email của mình. Bọn phisher hiểu rất rõ thực tế này nên đã lợi dụng chúng. 5. Sao tôi lại cần phải hành động để bảo vệ mình và công ty của mình khỏi email phishing cơ chứ? Đây là điều hoang tưởng cuối cùng và có lẽ cũng là quan trọng nhất. Người sử dụng luôn nghĩ rằng họ chẳng cần phải làm gì cả, hoặc làm cũng chẳng được ích gì. Thế nhưng, sự "lười biếng" này có thể dẫn tới hậu quả khôn lường: đánh mất thông tin cá nhân, tài chính và cả dữ liệu tối mật của công ty nữa. Theo dự đoán của MailFrontier, số tiền mà bọn phisher lừa đảo được trong năm nay sẽ tăng 25% so với năm ngoái lên... 1 tỷ USD. Cẩm Thi