PHISHER LỢI DỤNG TÀI KHOẢN IM ĐỂ LỪA ĐẢO

Thủ đoạn mới nhất của những kẻ lừa đảo trực tuyến (phisher) là đi ăn cắp tài khoản tin nhắn tức thời (IM) của người dùng Internet để đi lừa lừa người khác cung cấp thông tin cá nhân của họ. Các chuyên gia bảo mật đánh giá đây là một thủ đoạn vô cùng

Thủ đoạn mới nhất của những kẻ lừa đảo trực tuyến (phisher) là đi ăn cắp tài khoản tin nhắn tức thời (IM) của người dùng Internet để đi lừa lừa người khác cung cấp thông tin cá nhân của họ. Các chuyên gia bảo mật đánh giá đây là một thủ đoạn vô cùng hiểm độc. Nó là một phần trong nỗ lực nhằm tự trang bị cho mình nhiều nhiều công cụ tấn công người dùng Internet hiệu quả hơn của bọn lừa đảo trực tuyến. Chiếm đoạt được tài khoản tin nhắn tức thời của người khác sẽ là một công cụ có thể nói là rất hữu hiệu đối với bọn lừa đảo trong việc phát tán 'mồi nhử' của chúng. Các chuyên gia bảo mật đánh giá tỉ lệ thành công nếu sử dụng tin nhắn tức thời để lừa đảo có thể sẽ rất cao bởi tin nhắn tức thời mang tính chất cá nhân. Một phần nữa là tâm lý của người dùng dịch vụ tin nhắn tức thời, họ thường cho rằng chỉ những người bạn của mình mới biết nick chat của họ và mới có thể gửi tin nhắn cho họ. Chính vì thế mà nếu có nhận được tin nhắn 'mồi nhử' của bọn lừa đảo thì tỉ lệ người dùng Internet nhắp chuột vào những được liên kết trong đó là tương đối cao. Các hình thức tấn công lừa đảo trực tuyến truyền thống như gửi spam email giả mạo như là email hợp pháp của một tổ chức cá nhân nào đó đến hòm thư người dùng Internet vào lừa họ nhắp chuột vào các đường liên kết trong đó giờ đây đã không còn đạt được hiệu quả cao nữa khi mà người dùng ngày càng được cung cấp nhiều thông tin và được đào tạo để nhận biết những email dạng này. Ngày thứ sáu tuần trước đã có một nhân viên của Yahoo phát hiện ra là bọn lừa đảo trực tuyến đã sử dụng tài khoản tin nhắn tức thời của cô để gửi đường liên kết đến một trang web lừa đảo tới mọi thành viên trong danh sách liên lạc Yahoo Messenger của cô. Có lẽ những kẻ lừa đảo trực tuyến đã chiếm đoạt được tài khoản Yahoo Messenger của cô trong một chiến dịch lừa đảo khác. Trang web được gửi đi trong vụ tấn công lợi dụng tài khoản Yahoo Messenger của chính nhân viên Yahoo là một trang web được lưu trên dịch vụ web miễn phí Geocities cũng của Yahoo. Trang web giả mạo đó có hình thức trông rất giống với trang web Yahoo Photos và yêu cầu người dùng phải nhập tài khoản đăng nhập Yahoo. Nhà cung cấp dịch vụ Yahoo đã nhanh chóng loại bỏ trang web này. "Đây là những kẻ vô cùng hiểm độc. Chúng tôi phải nỗ lực ngăn chặn chúng bằng tất cả khả năng của chúng tôi," đại diện của Yahoo khẳng định. Giáo dục đóng một vai trò vô cùng quan trọng trong việc ngăn chặn lừa đảo trực tuyến qua tin nhắn tức thời, đại diện của Yahoo nói. Người dùng cần phải biết là không nên quá tin tưởng vào các tin nhắn tức thời nhất là những tin nhắn có chứa một đường liên kết bởi đó có thể là một đường liên kết đến những trang web độc hại, lừa đảo hoặc có chứa virus. Lừa đảo trực tuyến (phishing) là một hiểm hoạ bảo mật đang ngày càng trở nên phổ biến trên Internet. Trong tháng 8 vừa qua, đã có tổng cộng hơn 26.150 trang web phishing được tổ chức Anti-Phishing Working Group phát hiện.

Hoàng Dũng