 Đến hẹn lại lên, mỗi dịp Giáng sinh và năm mới, trên mạng Internet và viễn thông lại có khá nhiều "cạm bẫy" giăng lưới khách hàng. Người dùng cần cẩn trọng trước những chào mời có vẻ như rất hấp dẫn này…

Cảnh giác với email phát tán virus, spam

Cuối năm luôn là dịp để hacker lợi dụng tấn công người sử dụng. Giả mạo các thiệp điện tử chúc mừng ngày lễ hoặc các chương trình bán hàng khuyến mãi, hacker có thể lừa người sử dụng nhẹ dạ mở các file virus đính kèm trong email hay click vào các được link độc hại. Các email gửi e-card chúc mừng vào các dịp này không rõ nguồn gốc có chứa các mã độc hại

Người sử dụng cần cẩn trọng khi truy cập Internet trong dịp cuối năm, đồng thời cần trang bị cho mình phần mềm diệt virus thường xuyên cập nhật bản mới để bảo vệ cho máy tính và dữ liệu của mình. Năm ngoái, vào dịp này, hàng loạt email chứa mã độc khai thác giáng sinh đã phát tán.
Những email này giả mạo chiến dịch khuyến mãi của Cocacola nhân dịp giáng sinh với nội dung rất hấp dẫn: "Hãy thử sức với trò game online tuyệt vời của chúng tôi để có cơ hội trúng một chuyến đi tới Bahamas và uống Coca Cola miễn phí suốt đời. Xem file đính kèm để biết thêm chi tiết". Khi chạy file đính kèm, máy tính của người sử dụng sẽ bị nhiễm một backdoor và hacker có thể điều khiển máy tính của nạn nhân từ xa, cũng như đánh cắp các dữ liệu quan trọng.

Để bảo vệ máy tính trước những đợt tấn công lừa đảo này, người dùng cần luôn cảnh giác trước các thông tin hấp dẫn về ngày lễ tết dịp cuối năm. Ngoài ra, cần cập nhật phần mềm diệt virus phiển bản mới nhất, đồng thời không nên mở các file đính kèm không rõ nguồn gốc, đặc biệt là các file có đuôi .exe .com .pif .scr và .bat.

Ngoài các email không rõ nguồn gốc, các cư dân mạng cũng nên cảnh giác với trò lừa đảo để lấy thông tin cá nhân và mật khẩu blog Yahoo 360 qua mạng, thậm chí cả những thông tin trên Google.

Trong tháng 11 vừa qua, còn một "cạm bẫy" khác mà khá đông người dùng Internet mắc phải đó là Google bị lợi dụng làm phương tiện phát tán virus. Hầu hết người sử dụng Internet đều có thói quen tìm kiếm thông tin qua Google. Đó là lý do khiến hacker luôn tìm cách cài mã độc vào các từ khóa được tìm kiếm nhiều nhất trên công cụ này, biến Google trở thành kho phát tán virus khổng lồ.

Những sự kiện thu hút sự quan tâm của công chúng trên toàn thế giới và cả ở Việt Nam như Halloween, World Cup... luôn là điểm ngắm của hacker. Kẻ xấu liên tiếp dựng lên nhiều website chứa virus và sử dụng những kỹ thuật tinh vi đẩy đường link các website đó lên những kết quả tìm kiếm đầu tiên trong Google, vị trí mà người tìm kiếm dễ bấm vào nhất. Ngoài những sự kiện nóng, khi tìm kiếm các phần mềm, video clip, file nhạc hay thông tin về những nhân vật nổi tiếng thế giới... người sử dụng đều có thể bị dẫn đến những website chứa virus.

Tin nhắn lừa đảo cũng… vào mùa

Đến hẹn lại lên, cứ mỗi dịp cuối năm lại xuất hiện xu hướng gia tăng các tin nhắn lừa đảo nhắm đến người dùng di động tại Việt Nam. Phía cơ quan chức năng cũng thừa nhận, việc ngăn chặn và xử lý tin nhắn lừa đảo cần được tiến hành bằng cách phối hợp nhiều giải pháp với sự tham gia của nhiều bên có liên quan.

Tuy nhiên, vấn đề nhận thức của người dùng đóng vai trò rất quan trọng. Đây được cho là yếu tố then chốt và cần được ưu tiên tiến hành sâu rộng để ngăn ngừa các thiệt hại có thể xảy ra cho người dùng di động tại Việt Nam.

Các chuyên gia an ninh mạng khuyến nghị các thuê bao di động cần đề cao cảnh giác với các tin nhắn được gửi đi

từ những số thuê bao có dạng 01xxxxxxxxx, 09xxxxxxxx, số điện thoại cố định. Đặc biệt cảnh giác với những tin nhắn có nội dung thông báo trúng thưởng, tặng quà miễn phí, những tin nhắn gửi yêu cầu người dùng soạn tin nhắn gửi về các đầu số có dạng 6xxx, 8xxx để tham gia.

Thường, tin nhắn "dụ" gửi lại vào các đầu số là một trong các kiểu tin nhắn lừa đảo. Khi gửi tin nhắn cho các đầu số, người dùng nhớ lưu ý về giá cước khi gửi tin nhắn của mỗi đầu số của các nhà cung cấp dịch vụ nội dung để tránh mất tiền ngoài ý muốn.

Theo VNMedia