

VÌ SAO BẠN BỊ "NHỎI" E-MAIL SPAM?

Mỗi ngày mở hòm thư điện tử ra bạn thấy rất nhiều những bức thư lạ không biết của ai. Có những bức thư được gửi đi với nội dung quảng cáo, nhưng cũng có những bức thư không có nội dung gì cả. Bạn băn khoăn không hiểu làm sao những người này biết được địa chỉ email của

Mỗi ngày mở hòm thư điện tử ra bạn thấy rất nhiều những bức thư lạ không biết của ai. Có những bức thư được gửi đi với nội dung quảng cáo, nhưng cũng có những bức thư không có nội dung gì cả. Bạn băn khoăn không hiểu làm sao những người này biết được địa chỉ email của bạn khi mà bạn chỉ cho một số người địa chỉ email của bạn mà thôi. Đó chính là cái được gọi là SPAM - những bức thư rác. Nhưng làm thế nào SPAM biết được địa chỉ email của người dùng Internet? SPAM đã được gửi đi như thế nào? Trong bài viết này chúng tôi sẽ giúp bạn tìm hiểu rõ hơn về một vấn nạn của Internet. Đó là SPAM. SPAM là gì?

Thư rác, một vấn nạn của Internet.

SPAM thực sự gây ra rất nhiều khó chịu cho người dùng Internet, nhất là khi nó được gửi đi với số lượng lớn. Hàng ngày một địa chỉ email có thể phải nhận rất nhiều email SPAM cho dù có sử dụng một bộ lọc SPAM tốt đi chăng nữa. Tuy nhiên, SPAM nổi tiếng là thế, nhưng cũng có không ít người không biết thực sự SPAM là gì. SPAM là những email không được sự cho phép của người nhận (Unsolicited email) được gửi đi với số lượng lớn tới hòm thư của người dùng Internet. SPAM đôi khi còn được xem là những email thương mại không được sự cho phép của người nhận (UCE - Unsolicited Commercial E-Mail). Tuy nhiên, không phải mọi vụ gửi SPAM đều là nhằm mục đích quảng cáo thương mại. Một số vụ gửi SPAM lại nhằm mục đích bất chính hoặc cũng có những kẻ gửi SPAM chỉ để bày tỏ quan điểm chính trị hoặc tôn giáo. Hình thức gửi SPAM nguy hiểm nhất là hình thức gửi đi những thông điệp để lừa người dùng tiết lộ thông tin tài khoản ngân hàng trực tiếp, số thẻ tín dụng ... - hay đây chính là một dạng phổ biến của lừa đảo trực tuyến. Nguồn gốc của SPAM

SPAM là một tai họa đối với thư điện tử và nhóm thảo luận (newsgroup) trên Internet. SPAM có thể gây trở ngại đến sự hoạt động của các dịch vụ công cộng. Đây là chúng ta còn chưa nói đến tác động của nó đối với hệ thống email. Những kẻ chuyên gửi SPAM lấy đi những nguồn tài nguyên của người dùng và nhà cung cấp dịch vụ mà không phải đền bù bất cứ cái gì." (Vint Cerf – Cha đẻ của Internet)

Một trong số những vấn đề nhức nhối của SPAM đồng thời cũng là nguyên nhân lý giải tại sao lại có SPAM là “để tạo ra SPAM hay trở thành SPAMMER là một điều quá dễ dàng”. Bất cứ ai cũng có thể trở thành SPAMMER. Ví dụ, bạn có một món hàng độc đáo cần bán ngay. Nhưng để mọi người biết đến món hàng đó thì bạn phải làm thế nào. Bạn quyết định trước hết phải thông báo cho bạn bè biết bằng cách gửi email cho 100 người nằm trong sổ địa chỉ của bạn. “Wow!” bạn nghĩ “thế là mình không mất một đồng nào mà vẫn có thể gửi đi 100 email quảng cáo sản phẩm của mình. Nếu có người biết để mua hàng mình sẽ lời to. Tại sao mình không gửi email cho nhiều người khác nữa? Mình sẽ có thể thu được nhiều lợi nhuận hơn?” Rồi bạn sẽ tìm tòi ứng dụng các giải pháp để gửi đi được nhiều email cho cả những người bạn không quen biết hơn. Vậy là bạn đã trở thành SPAMMER. Đó mới chính là vấn đề thực sự của SPAM. Nó quá dễ để ai cũng có thể gửi đi trong khi chi phí bỏ ra chẳng đáng là bao, có khi là chả mất đồng nào. Và cho dù tỉ lệ bán hàng quảng cáo không cao, nhưng SPAM vẫn có một sức hút đặc biệt với giới tiếp thị. Gửi SPAM như thế nào? Để gửi SPAM, SPAMMER thường phải đi qua 2 bước cơ bản: Thu thập địa chỉ email và Gửi SPAM.

1. Thu thập địa chỉ email

Những kẻ chuyên gửi SPAM – hay còn gọi SPAMMER – có rất nhiều cách để thu thập địa chỉ email. Phổ biến nhất là những cách sau đây:

Cách thứ nhất là thông qua nhóm thảo luận (newsgroups) hoặc phòng chat (chat rooms) trên Internet, đặc biệt là các trang web cổng thông tin điện tử như AOL hay Yahoo. Với những dịch vụ như thế người dùng thường vẫn sử dụng địa chỉ email thực để đăng ký tài khoản. SPAMMER chỉ cần dùng một phần mềm đặc biệt là đã có thể lấy được địa chỉ email của rất nhiều người.

Cách thứ hai là khai thác trực tiếp từ Web. Hiện đã có tới hàng triệu trang web trên Internet và SPAMMER chỉ cần sử dụng các phần mềm tìm kiếm có khả năng lần tìm ký tự @ trong các trang web – như bạn biết, đây là ký tự đại diện cho địa chỉ email. Kết quả là SPAMMER cũng dễ dàng có được vô vàn các địa chỉ email trong tay. Những phần mềm như vậy thường được gọi là các SPAMBOT. Một cách khác là SPAMMER tạo ra các trang web đặc biệt chuyên dùng để thu thập địa chỉ email. Ví dụ, SPAMMER có thể tạo ra một trang web với tựa đề “Win \$1 million!!! Just type your e-mail address here!” (Bạn đã trúng giải thưởng 1 tỉ USD!!! Hãy để lại địa chỉ email của bạn!). Đã có không ít người trở thành nạn nhân của trò lừa đảo này. Hậu quả là hòm thư của họ đã bị chất đầy thư rác.

Chuyện thư rác đầy ắp hòm thư email không chỉ còn là chuyện xứ người, mà đã phổ biến cả ở Việt Nam.

Hay có những trang web tạo ra danh sách lựa chọn email "Would you like to receive e-mail newsletters from our partners?" (Bạn có muốn nhận tin thư từ đối tác của chúng tôi không?) Nếu bạn trả lời "Yes" thì ngay lập tức địa chỉ email của bạn sẽ được bán cho SPAMMER. Hoặc SPAMMER có thể thành lập một trang web cho đăng ký thành viên sử dụng, mà yêu cầu cung cấp địa chỉ email xác thực là yêu cầu cốt lõi của việc đăng ký. Trên thực tế đó chỉ là một cách để thu thập địa chỉ email. Trước đây, đã từng có rất nhiều các trang web lớn rao bán địa chỉ email của các thành viên. Có lẽ cách thức phổ biến nhất chính là cách thức được gọi là "dictionary attack". Đây là phương thức liên quan đến việc lập trình cho một chiếc máy tính có thể tạo ra rất nhiều biến thể từ một địa chỉ email bằng cách thay đổi các ký tự - ví dụ mike1@yahoo.com, mike2@yahoo.com, mike3@yahoo.com... Có một mô tả "dictionary attack" như sau: "Dictionary attack sử dụng một phần mềm để tạo một kết nối đến một máy chủ thư điện tử để gửi lên hàng triệu địa chỉ email bất kỳ. Rất nhiều trong số những các địa chỉ đó chỉ là những biến thể của một địa chỉ email – ví dụ jdoe1abc@hotmail.com và jdoe2def@hotmail.com. Phần mềm đó sẽ kiểm tra xem địa chỉ email nào "còn sống", địa chỉ đó sẽ "lọt vào mắt xanh" của SPAMMER". Các thức cuối cùng và cũng là cách dễ nhất chính là việc mua một chiếc đĩa CD có chứa hàng trăm hàng nghìn các địa chỉ email từ các SPAMMER khác. Và rồi một khi SPAMMER có được một số lượng địa chỉ email tương đối, chúng sẽ trao đổi với các SPAMMER khác và sẽ có được nhiều địa chỉ email hơn. Chúng bắt đầu gửi SPAM. Gửi SPAM SPAMMER cũng có rất nhiều cách khác nhau để có thể gửi đi hàng nghìn hàng triệu các bức thư rác – hợp pháp có mà bất hợp pháp cũng có. Cách thứ nhất là SPAMMER phải bỏ tiền đầu tư trang bị cho mình rất nhiều hệ thống máy tính, modem và kết nối mạng Internet để gửi SPAM. Đây là một cách thức hoàn toàn hợp pháp nhưng có chi phí cao. Tuy nhiên, kết quả đem lại sẽ có thể là hàng chục nghìn đô la tiền lợi nhuận thu về. Cách thứ hai rẻ hơn nhiều nhưng lại bất hợp pháp và cũng là cách thức nguy hiểm nhất đối với người dùng. Đó là cách gửi SPAM thông qua những máy chủ uỷ nhiệm mở (open proxy servers). Nói đến phương thức gửi SPAM này thì cũng là nói đến cách thức SPAMMER bí mật đột nhập bắt cóc hệ thống máy tính của người khác để xây dựng một cái được gọi là botnet.

Zombie PC

Trước hết SPAMMER sẽ sử dụng công nghệ và các thủ đoạn cần thiết để bí mật cài đặt một phần mềm lên hệ thống của người dùng. Đó là phần mềm cho phép SPAMMER có thể kiểm soát được hệ thống máy tính của nạn nhân từ xa - hay nói một cách khác là SPAMMER đã bắt cóc được chiếc máy tính đó. Chiếc máy tính đó đã trở thành một thứ được gọi là "Zombie" (thây ma). Khi có nhiều Zombie, SPAMMER sẽ tiến hành xây dựng một hệ thống mạng các Zombie – hay đây chính là hệ thống mạng botnet. Đến đây cách thức thứ hai đã giống với cách thức thứ nhất, chỉ khác một

điều là SPAMMER không phải có tiền ra mua các hệ thống máy tính mà chúng đi “bắt cóc” máy tính của người khác. Cách thức gửi SPAM thứ hai cũng nói lên một điều là tại sao SPAMMER ngày nay lại trở thành một mối đe dọa đối với mọi người dùng Internet và tại sao SPAM cũng được xem là độc hại không kém gì các phần mềm độc hại khác như virus, sâu máy tính hay trojan. Bạn nên biết để có thể đột nhập thành công và bắt cóc hệ thống máy tính của người dùng thì SPAMMER phải sử dụng các kỹ thuật tấn công khai thác lỗi bảo mật không khác gì hacker hay các kiểu cách lừa đảo không thua kém gì các phisher. Phần mềm giúp SPAMMER tấn công và bắt cóc máy tính của người dùng từ xa cũng chính là các loại phần mềm độc hại virus, sâu máy tính hoặc trojan. Nói một cách khác giờ đây dường như không còn danh giới giữa hacker và SPAMMER nữa, SPAM trở thành công cụ phát tán virus, sâu máy tính, trojan và ngược lại chính những phần mềm độc hại đó là công cụ để gửi SPAM. Bạn tưởng tượng xem nhé với một lượng SPAM vô cùng lớn gửi đi trên toàn thế giới mỗi ngày thì nếu hệ thống máy tính của bạn trở thành một Zombie thì sao? PC của bạn sẽ liên tục phải gửi đi các email SPAM, đường truyền Internet và PC của bạn sẽ chậm đi rất nhiều vì mọi tài nguyên đều đã được SPAMMER khai thác sử dụng. Mặt khác đôi khi bạn còn có thể trở thành nạn nhân của các cơ quan bảo vệ pháp luật. Vì họ có thể dễ dàng phát hiện ra PC của bạn đã sử dụng trong các vụ tấn công gửi SPAM bất hợp pháp nhưng để phát hiện được SPAMMER thì lại là vấn đề rất khó. Bạn trở thành nạn nhân bất đắc dĩ. Bạn hay xem một SPAM KING – ông vua trong việc gửi SPAM – nói gì nhé: “Tôi chiếm quyền điều khiển tổng cộng 190 máy chủ email – 110 chiếc ở Southfield, 50 chiếc ở Dallas và 30 chiếc khác ở Canada, Trung Quốc, Nga và Ấn Độ. Mỗi chiếc máy tính đó có thể gửi đi 650.000 email mỗi giờ, tương đương với khoảng hơn 1 tỉ email một ngày.” Ngoài ra còn có những công ty được thành lập để chuyên nhận các hợp đồng nhận gửi SPAM với giá rẻ. Nhưng công ty này tuyên bố họ hoàn toàn không phải là SPAMMER vì những khách hàng của họ chấp nhận nhận những email do họ gửi đi. Những địa chỉ email như thế này thường được thu thập bằng cách thức thu thập địa chỉ email thứ 3 như đã nói ở trên. Chống lại SPAM

Cảnh báo thư rác bằng công cụ Spam Alarm.

Công nghệ tốt nhất để chống lại SPAM hiện tại là sử dụng các phần mềm lọc SPAM. Bạn có thể tìm được rất nhiều phần mềm lọc SPAM trên Internet, tốt nhất là bạn nên vào trang web như pcworld.com hoặc download.com để tải về những phần mềm này. Tuy nhiên, như bạn biết SPAMMER đôi khi còn quyền điều khiển hệ thống của bạn để gửi đi SPAM, chính vì thế mà phần mềm lọc SPAM chưa phải là tất cả. Bạn còn cần phải thường xuyên cài đặt các bản cập nhật bảo mật cho hệ điều hành để vá các lỗi bảo mật tránh bị SPAMMER khai thác tấn công, bạn còn cần thêm một phần mềm tìm diệt các phần mềm độc hại, và tốt nhất bạn nên cần thêm một phần mềm

tường lửa cá nhân. Nhưng cho dù công cụ nào đi chăng nữa cũng không thể bằng con người. SPAM đã được xem là vấn đề xã hội liên quan đến con người, vậy chỉ có con người mới có thể chống lại được nó. Bạn hãy thật sự cẩn thận khi sử dụng Internet và trang bị cho mình những kiến thức cần thiết về bảo mật và sử dụng Internet an toàn. Có như thế bạn mới tránh được SPAM và những hiểm họa khác trên Internet. Trang Dung