

¿Por qué sigue triunfando el spam?

Su bajo coste, las cláusulas de algunos contratos respecto a los datos del usuario y la optimización de la tecnología otorgan a esta práctica una enorme rentabilidad

El 80% del correo digital es spam. Afecta a los servidores, a los servicios, a la privacidad de los usuarios y a su salud mental. Afecta a billones de personas y colapsa las carreteras de la Información. Sólo por el spam, la Red es siete veces más lenta de lo que debería. Sus responsables son probablemente las personas más odiadas de Internet y, sin embargo, siguen enviando miles de millones de correos no solicitados cada día. ¿De dónde vienen? ¿A dónde van? Y, lo que es más importante, ¿por qué no nos dejan en paz?

Cómo protegerse del spam

Los 'spammers' ganan millones de euros al mes bombardeando a desconocidos con sus reclamos insidiosos porque el proceso apenas cuesta dinero y basta con un mínimo porcentaje de éxito para que el esfuerzo merezca la pena. Su táctica consiste en ganarse la atención del usuario, después su confianza y, finalmente (de una manera u otra) su dinero antes de desaparecer tan rápido como habían llegado.

Sin embargo, para evitar el spam basta con seguir una serie de normas que, si se aplican correctamente, reducirán sensiblemente la cantidad de correos basura recibidos:

- * No distribuir el correo en el IRC, los sistemas de mensajería instantánea o los juegos online. Las paredes virtuales también escuchan.

- * No entregar los datos alegremente para participar en encuestas o ver un vídeo en la Red. Comprobar que la empresa o servicio es de fiar.

- * Leer atentamente las condiciones de uso: muchas veces incluyen una cláusula en la que se permite la venta de los datos a terceros con finalidad comercial.

- *

Utilizar una cuenta de correo desechable ('pook mail') para suscripciones a listas de correo masivas y servicios en la Red. Utilizar a la vez una privada para el correo personal y no confiársela a nadie.

- * No publicar la dirección en la Red. Si es necesario, usar una imagen, código ASCII o sustituir la arroba y el punto por las palabras 'arroba' y 'punto'. Cualquier cosa menos la dirección y el dominio. Millones de robots trabajan día y noche para hacerse con esos datos.

- * No enviar ni contestar 'correos cadena'. Además de comprometer el propio correo, se destapa también el de los demás. Si es imprescindible enviar un correo a varias personas a la vez; mejor utilizar la copia oculta.

- *

No abrir correos de desconocidos; siempre es mejor eliminar los correos sospechosos sin abrir.

- *

Nunca se deben abrir archivos adjuntos, especialmente si son ejecutables: son fuentes de infección del ordenador y de programas espía.

* No responder al correo publicitario no solicitado, aunque se ofrezcan a eliminar la dirección del usuario de su base de datos si se responde. Comprobar primero que la fuente es verídica y enviar una protesta formal si han enviado publicidad sin permiso.

* Utilizar filtros de spam efectivos y actualizados. Las cuentas de correo webmail suelen permitir configurarlos.

* Utilizar los recursos disponibles en el sistema para generar listas negras (direcciones IP y dominios) de spam. De este modo no sólo se elimina de la bandeja, sino que se contribuye a limpiar la Red.

Spam o 'no spam': he aquí el dilema

El Spam es cualquier información que llega al correo personal sin haber sido solicitada o aceptada previamente. Es una definición problemática, porque reúne en el mismo saco a los vendedores de Viagra y a los que solicitan ayuda para zonas en desgracia, pero no es el propósito sino el proceso lo que define al Spam.

Muchas empresas venden las bases de datos con las direcciones de sus clientes y usuarios a subcompañías y asociados, que las utilizan para promocionar sus propios productos. Aunque molesta, esta práctica puede ser legítima si el contrato firmado con ellos incluye una cláusula que se lo permite. Técnicamente, el usuario ha aceptado la venta de sus datos a terceros y, por tanto, lo que le manden no será Spam, aunque no sea correo deseado.

Otras veces, el origen del spam es una organización humanitaria que utiliza todos los recursos a su alcance para hacer su labor lo más eficaz posible. Su intención puede ser loable y su causa lo suficientemente importante como para que el medio justifique el fin. Pero eso no lo hace menos Spam.

Sociología del spam

El Spam se distribuye rápidamente gracias a la tecnología. Sin embargo, la tecnología no basta para que el 'spammer' consiga lo que quiere: se necesita también de la colaboración del usuario. Por eso todas sus tácticas están basadas en técnicas milenarias de marketing tradicional, siendo la más habitual jugar con los deseos ocultos de su posible comprador.

Spam y deseos secretos

Esto resulta fácil porque los deseos son mucho menos secretos de lo que al usuario le gustaría pensar. Más o menos todo el mundo fantasea con mejorar su estatus social, conseguir un trabajo mejor pagado (o hacerse rico sin trabajar), aumentar su atractivo físico, aumentar la potencia sexual, tener encuentros con desconocidos...



Hay miles de objetos, técnicas y fármacos milagrosos que prometen todas estas fantasías con la máxima discreción a través de la Red, ya que mucha gente se avergonzaría de comprar determinadas cosas en una tienda. De entre la gran maraña de spam, éste es el más pesado pero también el menos peligroso porque, al final, todo se reduce a un simple intercambio comercial.

En su ensayo 'Spam, the Economy of Desire', Alessandro Ludovico confirma que uno de cada 10.000 mails se convierte en una venta. Si consideramos la inversión inicial (un ordenador conectado a Internet y una persona frente al teclado) y que el mensaje tarda sólo dos horas en llegar a un millón de buzones, se puede empezar a comprender mejor el negocio. El principal objetivo de los spammers' no es hacerle la vida imposible al usuario, sino que lo que quieren es forrarse.



Spam y timo

En otros casos, el 'spammer' avisa de un negocio 'secreto', de un trabajo extraordinario o una situación a la que se puede sacar un provecho económico, como comprar objetos de lujo a precio de ganga o adquirir acciones en una empresa que sube como la espuma. En todos, la comunicación entre el spammer y su víctima se siente como cercana y personalizada, aún cuando el mismo mensaje ha llegado a cientos de miles de personas al mismo tiempo.

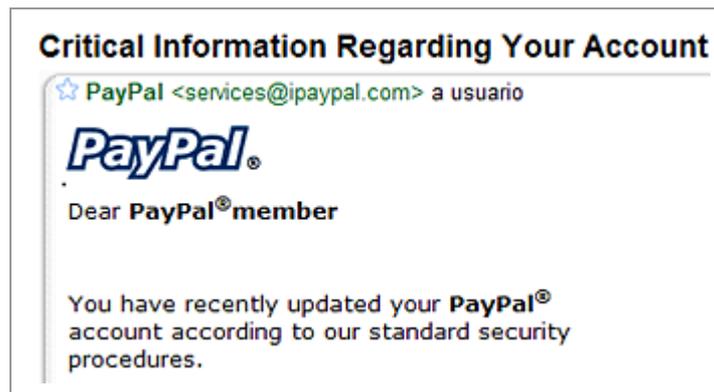
El asunto del mensaje es críptico y personal y muy a menudo parece un 'reenviado' que estaba dirigido a otro y que nos ha llegado por error. La táctica es recrear la sensación de que uno se encuentra un billete de lotería y que debe actuar deprisa antes de que el responsable se dé cuenta del error. La intención de estos 'spammers' es, en el mejor de los casos, conseguir que el receptor responda al mensaje y comprobar que la dirección es real. En el peor, estafar.

Si el usuario confirma su existencia, será incluido en una lista de correos válidos y recibirá veinte veces más spam que antes. Si facilita información más comprometida, como cuentas bancarias o el número de su tarjeta de crédito, su dinero desaparecerá mucho más deprisa de lo que tardó en ahorrarlo.

La única manera de reducir este tipo de spam es utilizar un buen filtro, particularmente aquellos que funcionan como las etiquetas, o 'tags', de la web 2.0: cada vez que se etiqueta un mensaje como 'spam', el sistema lo almacena y estudia sus características. Cuantos más mensajes se le dan, más información tiene para reconocer el spam y eliminarlo antes de que sea leído por el usuario.

Spam y 'phishing'

Otro tipo de spam diseñado para conseguir información confidencial del usuario está relacionado con las técnicas de 'phishing'. Su propósito es alarmar a la víctima con advertencias sobre su cuenta bancaria, su dominio o un servicio de comercio en la Red, como su cuenta de Amazon o Paypal, tal como se ve en el siguiente ejemplo:

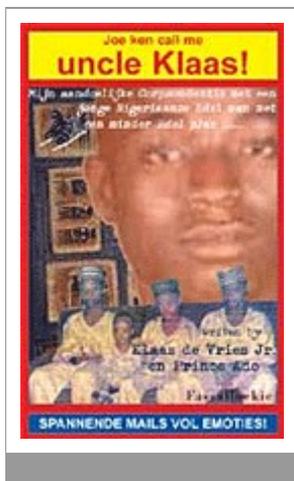


Su munición es sembrar la duda y el miedo: ha habido un problema de seguridad en el sistema y el usuario debe confirmar sus datos si no quiere perder su cuenta, su dinero o arriesgarse a ser suplantado por un estafador.

La única política posible con estos mensajes es denunciarlos y eliminarlos; ningún banco solicitará información delicada por correo electrónico y, si hay algún problema con el servicio en Amazon o Paypal del usuario, éste será advertido cuando entre en su perfil de usuario y nunca por e-mail.

Este tipo de estafadores son difíciles de localizar porque aprovechan agujeros de seguridad en servidores ajenos para cometer sus crímenes sin dejar huellas.

Spam y avaricia



En la misma línea, una de las estrellas más comentadas de la Red es el 'heredero nigeriano' (otras veces 'la viuda de un dictador asiático' o similar) que solicita la ayuda del receptor para mover una importante suma de dinero a cambio de un suculento porcentaje.

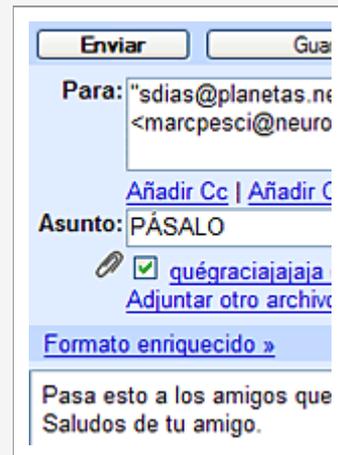
Este tipo de spam es el equivalente contemporáneo del 'timo de la estampita' y juega con la avaricia de la víctima para conseguir el número de su cuenta bancaria o una pequeña inversión. No hace falta decir que ha sido utilizado con éxito más de una vez y que siempre acaba mal para el usuario.

Como demuestran estos casos, la tecnología no lo es todo: el spam requiere de una respuesta activa por parte del receptor para conseguir lo que desea. Como afirma [Kevin Mitnick](#), el hacker más famoso de todos los tiempos, "la confianza es el camino al engaño". La tecnología facilita el trabajo al estafador pero, en última instancia, lo que tiene que conseguir es la confianza del usuario. La única manera de librarse del spam es desconfiar de desconocidos y utilizar el correo lo menos posible para enviar información confidencial.

El spam de los amigos

Hay un tipo de spam del que se habla poco y que, sin embargo, tiene una gran influencia en la bandeja del correo: el mail en cadena. Ocurre cuando una persona tiene algo gracioso, curioso o interesante que mostrar y lo envía de un solo golpe a todas sus direcciones de correo.

Tanto si es información sobre la deforestación del Amazonas como fotos de las vacaciones en Grecia, este tipo de correos no sólo consumen el ancho de banda, ralentizan las comunicaciones y malgastan el tiempo del usuario, sino que son utilizados por los 'spammers' para recoger direcciones de correo activas y venderlas al mejor postor. Lo más inteligente es no participar y pedir a los amigos que eviten ese tipo de 'cadenas' o que, si resulta estrictamente necesario, utilicen la línea de copia oculta.



¿Cómo nació el spam?

El spam, tal y como se lo conoce, vio la luz por primera vez en 1978. El uno de mayo de ese año, el departamento de marketing de DEC (fabricante de ordenadores) invitó a todos los usuarios de [Arpanet](#) de la costa oeste americana a la presentación de su nuevo modelo de DECSYSTEM-20 en Los Angeles y San Mateo.



Aunque era información que necesariamente interesaría al selecto grupo de pioneros de la Red (la mayoría relacionados con la informática y las comunicaciones) la invitación fue mal recibida por dos motivos principales. El primero, porque no había sido solicitada; el segundo, porque se había utilizado el correo personal de los usuarios sin haber recibido su permiso previo.

Parece un poco exagerado por parte de los usuarios de Arpanet, pero es importante recordar que, con el abuelo de Internet, la velocidad de transmisión de datos y la capacidad de los servicios era infinitamente más limitada que la existe ahora, por lo que las normas de etiqueta eran muy estrictas en cuanto a qué, cómo y cuánto era lícito enviar.

El spam, tal y como se lo conoce, vio la luz por primera vez en 1978

Curiosamente, uno de los pocos 'invitados' que defendió a la empresa fue [Richard Stallman](#), programador y pionero del software libre, y lo hizo en términos de libertad de expresión. Más adelante lo criticó, no por atentar contra la intimidad sino por hacerlo contra la etiqueta: el 'asunto' del correo era demasiado largo para ser aceptable.

Etimología del spam

La palabra spam es la abreviatura de 'Spiced Ham', un infame producto de carne

enlatada de muy baja calidad introducido por 'Hormel Foods' en 1937. Por su precio y conveniencia (no necesita nevera) alcanzó una rápida popularidad en el mercado americano y alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial. En los años 60, 'Hormel Foods' introdujo la anilla de apertura automática, eliminando la necesidad de abrelatas.



La cima de su popularidad fue retratada cómicamente en un sketch del grupo británico [Monty Python](#) en el 25 episodio de The Flying Circus. En dicho [sketch](#), lanzado el 15 de diciembre de 1970, un grupo de vikingos entra en una cantina británica y trata sin éxito de pedir una combinación de alimentos que no incluya Spam. Mientras el actor Terry Jones vestido de camarera les canta el menú, resulta evidente que su misión es imposible y la escena termina con todo el bar coreando al unísono "Spam, spam, spam, spam. ¡Rico spam! ¡Maravilloso spam! Spam, spa-a-a-a-am, spa-a-a-a-a-am".

La pareja de abogados Laurence Canter y Martha Siegel mecanizaron el proceso bombardeando las listas de Usenet para anunciar sus servicios

La palabra 'spam', mencionada 94 veces, inspiró a Joel Furr (una de las primeras estrellas de Arpanet) para bautizar el envío masivo de información no solicitada en la Red en marzo de 1993. Justo un año más tarde, la pareja de abogados Laurence Canter y Martha Siegel mecanizaron el proceso bombardeando las listas de Usenet (las primeras listas de correo) para anunciar sus servicios.

Sentaron un mal precedente: en menos de 24 horas, la firma facturó casi 10.000 dólares en casos y el 'Floodgate Bulk Email Loader' (un sistemas de envíos de correos masivo) se convirtió en el mejor amigo del 'spammer' y la pesadilla del resto de los usuarios de la Red.