COMBATIENDO AL ENEMIGO INVISIBLE:

El *"spam"* frente a la identidad digital

Carlos Macián Ruiz
Doctor Ingeniero de Telecomunicación

El 76% del correo que recibimos es *"spam"*: mensajes enviados de forma masiva, normalmente de carácter comercial, a menudo ilícitos y fraudulentos, que no hemos solicitado y preferimos no recibir. A escala mundial, su procesado supone unos costes elevadísimos a lo que hay que añadir el daño causado por los virus que a veces contienen, el robo de datos personales (*"phishing"*) y otros fraudes.

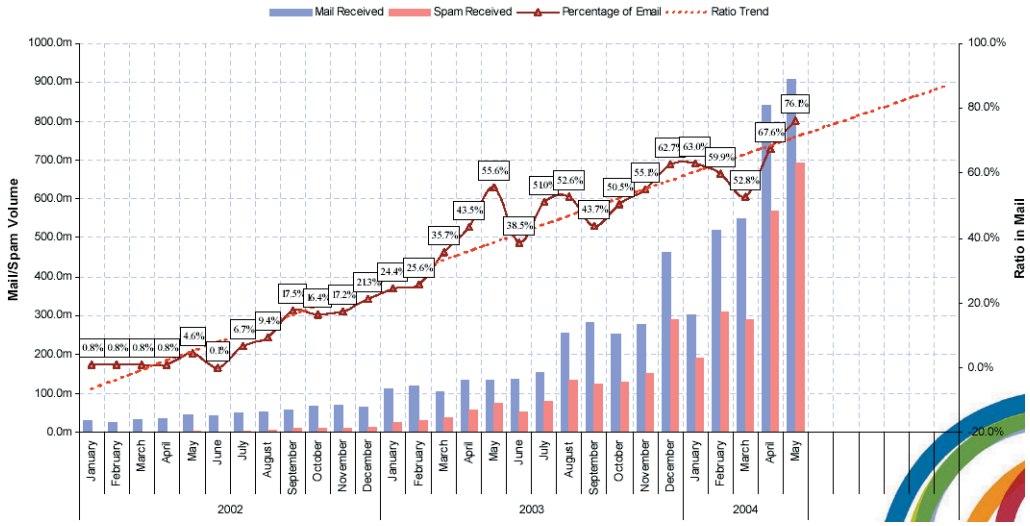
Cambiar de dirección de correo electrónico no es nunca una decisión cómoda. De entrada, hay que avisar a todos nuestros contactos habituales, tanto profesionales como personales, de nuestro cambio de dirección. Además, hay que asegurarse de mantener durante suficiente tiempo ambas direcciones activas, con el fin de no perder mensajes de interlocutores que se dirigen a nosotros por primera vez y sólo disponen de la información anticuada, o de contactos antiguos que no se han acordado de actualizar nuestra dirección. Cómo mínimo, hay que disponer de algún mecanismo de reenvío o de aviso de cambio de coordenadas.

Sin embargo, llegados a cierto punto, cambiar de dirección de correo electrónico es sencillamente una necesidad. Según datos recientes, el 76% del correo que recibimos es *"spam"*: Mensajes enviados de forma masiva, generalmente de carácter comercial, frecuentemente ilícitos o fraudulentos, y que nosotros no hemos solicitado y preferiríamos no recibir. Tres de cada cuatro. Se dice pronto.

El procesado de estos correos supone, según algunos estudios, unos costes de 10.000 millones de euros al año a escala mundial, y eso sin incluir el daño causado por los virus que a veces contienen, robo de datos personales (phishing) y otros fraudes. Diez mil millones sólo en los mecanismos necesarios para transportar, recibir, almacenar y procesar los billones de correos indeseados que diariamente recibimos. Y hay más: Se calcula que el *"spam"* conlleva una pérdida de productividad por trabajador y año cercana a los 1.500 euros. En castellano: El sueldo mensual neto de un ingeniero superior con algunos años de experiencia. O sea, que sólo rinde 11 meses al año, por culpa del *"spam"*.

Así pues, en algún momento nuestro buzón de correo está tan lleno de correos indeseados, a pesar de los filtros, listas negras y otras soluciones al uso, que uno se plantea "empezar de nuevo", disponer de una cuenta a la que sólo lleguen aquellos correos que realmente uno desea recibir. Pero inevitablemente, después de poco tiempo, nuestra nueva dirección cae en manos de los *"spammers"* y la pesadilla vuelve a comenzar.

Seguro que todos nos identificamos con este escenario, y seguro que, siendo ingenieros, nos hemos preguntado más de una vez cómo se puede evitar, o parar, esta plaga.



Pero para resolver el problema, primero hay que conocer sus causas. ¿A qué es debido el imparable crecimiento del *"spam"*? O dicho de otra manera, ¿por qué elige una persona convertirse en *"spammer"*? La respuesta se resume en cuatro palabras: Es sencillo, es barato, es rentable y además, es seguro.

Es sencillo, porque no hacen falta conocimientos especializados para mandar correos electrónicos de forma masiva: Basta un mínimo de dominio de la ofimática más básica.

Es barato, porque tanto los costes de establecimiento como los costes por correo enviado son muy bajos. La lista de la compra de un *"spammer"* primerizo podría lucir como sigue:

–Un PC: 800 € (con pantalla plana de 19 pulgadas incluida)
– Una lista de 20 millones de direcciones de correo donde enviar los primeros mensajes: 150 €
– El software para "recolectar" nuevas direcciones de las páginas web de empresas y particulares, para ampliar la lista inicial de direcciones: 40 €

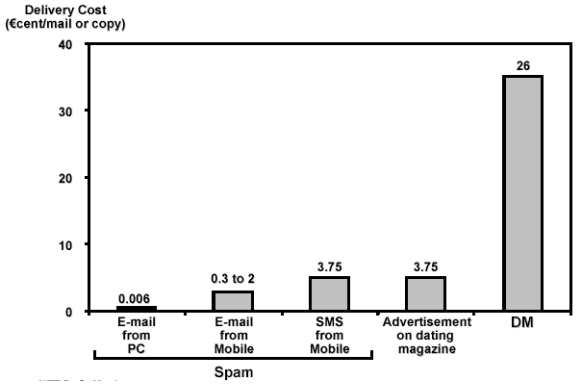
"Localizar al 'spammer', en un entorno de descoordinación internacional y falta de armonización en la legislación contra el 'spam', es una tarea que roza lo épico"

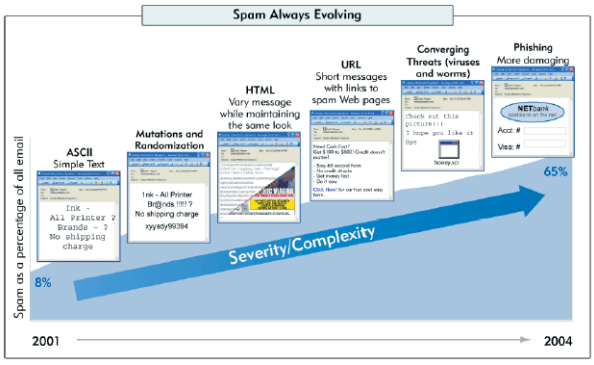
– Alquiler de una conexión de banda ancha, incluyendo quizá el hosting de los servidores, si así se desea: Unos 100 €/mes

Así pues, por unos 1.100 €, un internauta puede adquirir el kit básico de *"spammer"*, a través de la red y sin ni siquiera tener que realizar ninguna actividad ilegal. Pero es que además, el coste marginal de enviar un correo electrónico (teniendo en cuenta factores como el coste de la conexión de banda ancha, la amortización del hardware y del software, etc.) ronda los 0,04 céntimos de euro. Es decir, con una inversión de apenas 40 € se puede enviar 1.000.000 de correos electrónicos. Con tan magras necesidades de inversión, está claro que el *"spam"* es uno de los negocios más accesibles para cualquier persona, incluso aquellas que no disponen de acceso a líneas de capital al uso: Ciudadanos de pocos recursos, habitantes de países subdesarrollados, etc. En este sentido, el *"spam"* es uno de los negocios más universales y democráticos que existen.

Pero no nos hallaríamos ante una creciente comunidad *"spammer"* si no fuese rentable. Y para serlo, los sufridos destinatarios del *"spam"* han de reaccionar positivamente a esas ofertas de riqueza rápida, software a bajo precio o diversos aditamentos para la virilidad masculina. Y eso es lo realmente escalofriante: Por mucho que nuestra experiencia personal parezca desmentirlo, el *"spam"* se está convirtiendo en el mecanismo de marketing más eficiente del mercado! Algunos datos que lo atestiguan:

– Un 33% de los receptores de *"spam"* han seguido alguna vez





los enlaces a páginas web que éstos contienen

- Un 9% han contestado a dichos correos en alguna ocasión
- Un 3% han cedido información personal a requerimiento de un correo basura
- Un 5% han comprado en alguna ocasión los productos anunciados
- En EEUU, el 3,4% de la población ya ha sido objeto de intentos de fraude por suplantación de personalidad, eminentemente de bancos (phishing); de estos intentos, un 5% han tenido éxito.

Así pues, un 5% de las teóricas víctimas de esta terrible plaga han comprado en alguna ocasión los productos ofertados, o han caído en la trampa del phishing.

- Uno de cada veinte.
- Me atrevería a decir que pocas herramientas de marketing conocidas son tan efectivas.
- Si a la baja inversión necesaria le sumamos la alta tasa de éxito, queda claro que el *"spam"* es un negocio ilegal, pero altamente atractivo.

Y sin embargo, el *"spammer"* medio no es un criminal profesional al uso, perteneciente a, y protegido por, una potente organización mafiosa. Más habitualmente, se le consideraría un truhán de medio pelo, de esos que van buscando el dinero fácil y seguro. Y es aquí donde entra en juego la última variable de esta ecuación: El riesgo.

"La acción concertada mitigará el problema del *'spam'*. Jamás lo erradicará, salvo que ataquemos el talón de Aquiles de este negocio: La relación coste/beneficio"

El *"spam"* es un negocio seguro, por diversas razones. En primer lugar, porque la tecnología asociada al correo electrónico (el protocolo SMTP, los programas de correo y la propia tecnología de Internet) es inherentemente insegura: Nada tan sencillo como introducir una dirección de correo falsa como remitente de un correo. Y no sólo eso: Conseguir localizar al remitente físico de un correo electrónico es un proceso muy complejo, dado que generalmente el emisor se aprovechará del anonimato que concede Internet, usando direcciones IP dinámicas, accediendo desde ISP poco escrupulosos, a menudo sitos en terceros países, más permisivos con este tipo de actividades. Localizar al *"spammer"* en estas condiciones, en un entorno de descoordinación internacional y falta de armonización en la legislación contra el *"spam"* es una tarea que roza lo épico. Y aunque se le localizase, llevarlo frente a la justicia del país en el que ha cometido el crimen, que frecuentemente no será ni su pais de residencia, ni de nacionalidad, ni aquél en que su infraestructura se halla hospedada, es otra odisea para las autoridades involucradas. Y el *"spammer"* lo sabe.

¿No hay, pues, soluciones contra esta plaga? ¿Hemos de aceptarla como uno de los "efectos colaterales" de Internet? La respuesta tiene que ser, por supuesto, no. Hará falta una mezcla de medidas, todas ellas necesarias y ninguna suficiente, para combatirlo:

- Medidas técnicas, como filtros, mecanismos de reputación, limitadores de tasa de envíos, etc.
- Educación y concienciación de los usuarios y empresas del sector, de modo que sean conscientes de los peligros que se corren y de cómo combatirlos
- Una legislación adecuada, que claramente especifique los límí-

tes de la legalidad en el terreno de la publicidad online y qué medidas pueden tomarse contra los que las infrinjan
- Adecuados mecanismos de persecución de los criminales, de modo que la ley se haga cumplir
- Y por último reforzar la cooperación internacional, puesto que el *"spam"*, como otras formas de la actividad criminal dentro y fuera del ciberespacio, no conoce de fronteras; es más, se aprovecha de las diferencias y desacuerdos entre los Estados en su propio beneficio

Será una acción concertada en todos estos frentes la que nos acerque a la mitigación del problema, pero seamos sinceros: Nunca a su erradicación, excepto que se consiga atacar el auténtico talón de Aquiles de este negocio: La relación coste/beneficio. Y uno de los elementos fundamentales de esa relación es el anonimato, puesto que el anonimato garantiza la impunidad al *"spammer"*. Y es aquí donde los sistemas de autenticación electrónica y los mecanismos de identidad digital pueden jugar un papel muy destacado.

Iniciativas como el DNI digital pretenden hacer las transacciones en Internet más seguras, entre otras cosas. ¿De qué modo serán más seguras? Básicamente, porque podremos estar seguros de la identidad de aquél con el que realizamos las transacciones, dado que su DNI estará certificado por una de las pocas instituciones en las que todos, con más o menos matices, confiamos: La Administración Pública. Es decir, no será la identidad en sí lo que nos importe (si yo no conozco a Pepito Pérez, difícilmente podré saber si puedo o no fiarme de él, por mucho que sepa su nombre), si no el hecho de que podremos identificar fehacientemente a esa persona o entidad y llevarla ante los tribunales, en caso de fraude, incumplimiento de contrato o cualquier otro crimen. Y es precisamente esta característica la que modifica radicalmente la relación coste/beneficio del *"spammer"*: Si sus comunicaciones estuviesen necesariamente validadas por su identidad digital, avalada por la Administración Pública, el manto del anonimato bajo el cual opera se volatilizaría, y con él, su impunidad. Y sin impunidad, a un truhán de medio pelo quizá no le compense meterse en según qué negocios.

Vaya por delante que orquestar un mecanismo de este tipo no es trivial: Es preciso incluir mecanismos de autenticación basados en el DNI digital en los programas de correo habituales, cosa que requerirá tiempo; educar a los usuarios, adaptar los equipos, etc. Y además, tampoco se trata de una piedra filosofal: También hay DNI falsos hoy en día, y además el *"spammer"* podrá seguir operando desde el extranjero para garantizarse, si no la impunidad que da el anonimato, al menos sí una importante ventaja para eludir la acción de la justicia del país ofendido. Es decir, eliminar el anonimato no resolverá el problema, pero hará el negocio mucho menos atractivo. Si a eso le sumamos las otras medidas mencionadas anteriormente (cooperación internacional, medidas técnicas, educación, etc.), estaremos ante un panorama mucho más halagüeño en nuestra lucha contra la pandemia del ciberespacio.

Así pues, bienvenido, DNI digital. Al dotar de identidad a los usuarios, solventa uno de los grandes déficits de Internet en la lucha contra el *"spam"*: El anonimato. Y si el *"spam"* decrece, mi buzón de correo, mi productividad, mi empleador y mis nervios lo agradecerán enormemente. ◆

"El DNI digital hará las transacciones en Internet más seguras porque estará certificado por la Administración Pública"