

Sobre “hoaxes”, leyendas urbanas y otros rumores



Juan J. Sánchez Aguila-Collantes

“El motivo de este mensaje es advertir a los usuarios sobre un nuevo virus que circula en Internet. El virus se llama jdbmgr.exe y se transmite automáticamente a través del correo electrónico. Este virus es altamente peligroso y ningún antivirus lo consiga detectar permaneciendo 14 días en letargo antes de dañar el sistema completo. Puede ser borrado antes de que elimine los archivos del disco duro del ordenador. El virus suele situarse en la carpeta XXX¹. Para eliminarlo, buscar el virus anterior (el icono tiene forma de osito) y borrar manualmente el citado fichero. No olvide avisar reenviando este mensaje a todas las personas que tenga en su libreta de direcciones antes de que cause algún daño. Gracias”

Ante un mensaje como el anterior. ¿Cuáles serían los posibles modos de actuación?:

- Reenviarlo inmediatamente a los amigos dada la gravedad del tema en cuestión.
- Desinfectar el ordenador siguiendo las instrucciones y avisar al mayor número de conocidos para que a su vez procedan a desinfectar sus ordenadores.
- Enviar el mensaje directamente a la papelería sin opción a reciclado.

Por si todavía no lo tiene claro, presentamos otra variante del anterior mensaje de aviso: “Soy el primer virus andaluz (léase madrileño, gallego o catalán en sus múltiples variantes). Este virus trabaja basándose en un sistema de honor. Borre todos los archivos de su disco duro manualmente y envíe este mensaje a todos los miembros de su lista de correo. Muchas gracias”.

¿Está ahora ya más clara la respuesta?. En cualquiera de los dos casos, podemos asegurar que nuestro ordenador no funcionará mejor (ni peor, pues directamente no funcionará) si seguimos las instrucciones al pie de la letra.

Todos hemos sido víctima en mayor o menor grado de los “hoaxes”. Pero ¿de qué se trata y como comportarse ante ellos?

Los denominados como “hoaxes” son mensajes con textos alarmantes o llama-

tivos, engañosos en cualquier caso, que se envían por correo electrónico con el propósito de alcanzar una difusión masiva.

Este fenómeno no es nuevo, y con anterioridad al mecanismo actual se solían enviar cartas por correo postal asegurando siempre la peor de las desgracias en el caso de cortar la cadena y prometiendo toda suerte de bondades en el caso de continuar el envío. Con el advenimiento del correo electrónico como medio eficaz de comunicación el fenómeno se ha disparado con mensajes cada vez más imaginativos, pero siempre engañosos, de la misma forma que el *spam* ha sustituido y amplificado los efectos de los envíos publicitarios comerciales por vía postal.

Precisamente en el “spam” se encuentra una de las claves de los *hoaxes*. Y es que uno de sus objetivos principales es obtener direcciones de correo electrónico (las de todos aquellos por los que ha pasado el mensaje) para engrosar la lista de los “spammers”, contribuyendo de este modo a congestionar servidores y redes y compartiendo así uno de los objetivos del *spam* en general.

Las consecuencias derivadas de todo ello son una pérdida de tiempo y dinero para el receptor, un aumento de la banalización de la Red con la consecuente pérdida de confianza en ella como tecnología de comunicación por parte de los usuarios, aunque por supuesto

no podemos olvidar la tan importante inyección de autoestima que los *hoaxes* producen en su autor.

Pero ¿cómo reconoceremos que un *hoax* es auténtico?

Todos estos mensajes suelen tener una serie de características comunes que los hacen fácilmente reconocibles y acreedores de su particular certificado de pedigrí:

- Siempre le pasaron a un amigo de un amigo (es lo que en inglés se denomina “friend of a friend tales” o FOFT) y nunca hay nadie que asegure que le ha sucedido personalmente, aunque extrañamente a veces pasa que hay personas que se suman a confirmar lo que allí se cuenta pese a ser falso.
- Siempre piden ser reenviadas. Precisamente para cumplir el objetivo para el que fueron creadas. Algunas de las historias más espectaculares parecen dar por supuesto su reenvío por lo que eliminan esta petición y por ende una de las pistas. Sin embargo las más flojas o las que menos credibilidad presentan necesitan recurrir al también característico *compendio de desgracias*, que se avencinarán sobre uno y cuyo número suele

¹ Aunque el mensaje es real, no reflejamos la carpeta por si algún lector de Bit tras leer este párrafo no continúa leyendo el resto del artículo, pero decide proceder a “eliminar el virus”

anunciarse como inversamente proporcional al de las personas a las que se reenvíe el mensaje.

- Aparecen misteriosamente y nadie sabe de donde salen, aunque a veces se suelen citar fuentes como la policía o medios de comunicación.
- Pueden incluir elementos de horror, peligro, sexo o en cualquier caso morbo (resorte efectivo a la hora de reclamar la atención en el género humano) e incluyen términos del tipo PELIGRO, HORROR, ESPELUZANTE... siempre rodeados por varios pares de admiraciones (!!).
- Están en el límite de la realidad. Son falsas pero pueden tomar elementos de la realidad y aunque son poco creíbles podrían ser ciertas.

Desde que se viene conociendo su existencia se han detectado diferentes variantes de *hoaxes* que, hasta la fecha, y teniendo en cuenta que con el tiempo podrán surgir nuevas, son las siguientes:

- Las cadenas de la suerte, mágicas o supersticiosas. Este es el tipo más primitivo y directamente derivado de la correspondencia postal. Estas suelen incluir al final el ya mencionado *compendio de desgracias*.
- Las alertas sobre peligrosos virus informáticos, ya sean verdaderos, falsos o “engañosamente verdaderos” como el visto en la introducción.
- Las cadenas de solidaridad, los anuncios de desaparecidos o peticiones. En este sentido conviene recordar el caso “Shergold”. Esten niño inglés al que se le diagnosticó cáncer terminal en 1989 pidió que sus amigos le enviaran tantas tarjetas como fuera posible para ostentar un record en el libro Guinness. Craig Shergold se recuperó dos años más tarde, y pese a haberse eliminado esta categoría del libro Guinness, aún recibe bastantes tarjetas postales al día que todavía hoy siguen colapsando a la oficina de correos. Esta historia verdadera se ha tomado como modelo de *hoax*, y suele ser frecuente que de vez en cuando aparezcan historias semejantes en la Red.
- Las leyendas urbanas. Ya saben, como aquella de los cocodrilos que, descendientes de un pequeño reptil arrojado al inodoro cuando sus dueños se



“No sea ingenuo, no va a recibir 1 euro por cada persona a quien reenvíe el mensaje, ni ninguna compañía de telefonía le va a regalar el último prototipo de terminal móvil”

- cansaron de tenerlo como mascota, pueblan hoy las cloacas de Nueva York.
- Los rumores propiamente dichos como tomaduras de pelo o engaños. No sea ingenuo no va a recibir 1 euro por cada persona a quien reenvíe el mensaje ni ninguna compañía de telefonía le va a regalar el último prototipo de terminal móvil).
- Y por último, los chistes, bromas y parodias en formato textual, gráfico, sonoro o vídeo.

Si hemos de hacer algunas recomendaciones, la regla de oro fundamental a seguir en estos casos es **No reenviar los mensajes**. No obstante si, bien porque el mensaje recibido fue lo suficientemente ingenioso, se dudase de su autenticidad o por si en algún caso se temiese al *compendio de desgracias* en caso de romper la cadena (insisto, la opción siempre más aconsejable en cualquiera de los casos), se decidiese finalmente reenviar a una lista de “amigos”, antes de hacerlo no estaría de más, si de verdad los consideramos como tales, hacer lo siguiente:

Primero deberíamos asegurarnos de que los destinatarios elegidos no vayan a pasar a engrosar la amplia lista de futuras víctima de *spam*, lo que incluso podría llevar también asociado la pérdida de esa condición de “amigo”. Pa-

ra ello es aconsejable realizar la difusión a una lista privada (o destinos en Bcc) de forma que en un momento determinado la cadena que se genere no sea visible y no se pueda utilizar para extraer direcciones de correo.

Pero si además de lo anterior queremos hacer un favor a un pobre grupo de internautas anónimos y potenciales ex-amigos de un sujeto de dedo fácil, un par de clicks de ratón bastarán para eliminar toda esa lista de direcciones de correo electrónico que precede al mensajito en cuestión y que nos revela el camino que ha traído antes de llegar a nosotros.

Para finalizar algunos ejemplos de “hoaxes”, además de los ya apuntados, que se han hecho famosos y del que alguno de ustedes quizás hayan oído hablar:

El falso caso de los “gatitos bonsai”, uno de los casos más elaborados, a la par que desagradables, pues además contaba con una web de apoyo en la que se aseguraba que podía hacerse un gatito en miniatura como si se tratase de un bonsai. Al final, como en otros tantos casos, demostró ser una broma de un estudiante aburrido.

Otros pasan por descubrir en las profecías de Nostradamus referencias a los atentados del 11 de septiembre, la historia de las bases secretas de OVNIS que Hitler poseía en la Antártida, la vinculación de Satán con el nombre de Bill Gates o del mismísimo número de la bestia embebido en los códigos de barras de cualquier producto y como no destacar esa verdadera función de los hornos microondas y que suele ser tan desconocida, la de dispositivos de control mental a disposición de los gobiernos! ¿Hay quien dé más?... Sí: El “Ase-rejé” parece ocultar en su letra un mensaje satánico.

direcciones

Hoaxbusters.ciac.org Motor de búsqueda de “hoax” y consejos para reconocerlos

<http://www.rompecadenas.com.ar/>
www.PePi-II.com

@rompecadenas
Iniciativa PePi-II

www.keteu.org/~haunma/shergold.html La historia de Craig Shergold

www.webcom.com/~pinknoiz/coldwar/microwave.html Microwave Mind Control

www.geocities.com/Heartland/Meadows/2360/tracts/666.html Warning: 666 is coming

vipx.telepolis.com/leyendasurbanas/famosos/asereje.htm El mensaje satánico oculto en el “Ase-rejé”

vipx.telepolis.com/leyendasurbanas/creencias/index.htm Algunos ejemplos de “hoaxes”