Bulo-Hoax

Chavez Salazar Cristian
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
cristian.c10@hotmail.com

RESUMEN

Los hoaxes (broma, engaño) son mensajes de correo electrónico engañosos que se distribuyen en cadena. Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que pueden sucederte si no reenvías el mensaje a todos los contactos de tu libreta de direcciones.

También hay hoaxes que tientan con la posibilidad de hacerte millonario con sólo reenviar el mensaje o que apelan a la sensibilidad invocando supuestos niños enfermos.

Hay otros que repiten el esquema de las viejas cadenas de la suerte que recibíamos por correo postal que te auguran calamidades si cortas la cadena y te prometen convertirte en millonario si la sigues.

Palabras Clave

Correo electrónico, cadenas, hoax, bulo.

1. INTRODUCCION

Un correo electrónico no deseado supone de por sí una pérdida de tiempo. Pero los hoax pueden ir un paso más allá y a través del engaño llegar a perjudicar seriamente al receptor.

El hoax por excelencia es el mensaje que advierte de los peligros de un virus informático. Puede simplemente crear una falsa alarma que se extiende sin freno entre la lista de contactos de los receptores e incluso recomendar acciones preventivas que ocasionen daños sobre la computadora.

Los virus son una amenaza real que padecen los usuarios de ordenadores, en especial aquellos que utilizan con frecuencia el correo electrónico. Ahí es donde los bromistas encuentran sus víctimas: las alertas de nuevos virus son una práctica diaria, por lo que el usuario se siente incapaz de discernir entre los avisos reales de los bulos.

Los creadores de hoax utilizan mensajes que emulan las alarmas reales, recurriendo a un lenguaje difícil de comprender y citando alguna fuente conocida, por lo general fabricantes de antivirus para hacer el texto más creíble. El usuario debe sospechar del tono alarmista, que a veces llega a extremos. Este es un ejemplo: "el virus borrará para siempre todo su disco duro" o "fundirá su monitor".

La variante más perniciosa de los falsos virus es aquella que además de advertir del peligro, recomienda al usuario tomar medidas de las que luego se arrepentirá. Lo normal es convencer al usuario incauto de que un archivo alojado en su equipo es un parásito y debe eliminarlo. Eligen un archivo presente de manera habitual en el sistema y apremian a borrarlo, por lo que el destrozo que pueden ocasionar es mayúsculo si el archivo elegido es imprescindible para el funcionamiento de la computadora.

Además de los hoax que alertan sobre amenazas virales, existen otros tipos de mensajes que comparten con éstos ciertas características. Estas son algunas:

Catastrofistas. Son bulos que advierten de los desastres inminentes, desde la posibilidad de que el teléfono móvil explote en las manos, hasta de un Apocalipsis cercano provocado por un escape radiactivo. Suelen citarse fuentes oficiales para dotarlos de credibilidad, pero es improbable enterarse de una amenaza real mediante un correo electrónico de procedencia dudosa antes que a través de las propias fuentes oficiales o mediante cualquier otro canal de comunicación.

Mensajes en cadena. Constituyen una auténtica perversión del correo electrónico, pues contribuyen a la extensión de informaciones falsas que crean alarma y saturan buzones, redes y servidores. Lo peor es que inutilizan el correo electrónico como medio eficaz para difundir comunicaciones de verdadero interés. Su contenido suele apelar a la conciencia del receptor -peticiones de ayuda para un enfermo terminal o para la localización de una persona desaparecida- o a su superstición -auguran toda suerte de parabienes a quien reenvíe el texto a una serie de personas-

Ofertas y trucos. Con el nombre de alguna compañía conocida en la cabecera, se informa de extraordinarias ofertas o de artimañas para, por ejemplo, recargar el teléfono móvil de forma gratuita. Aunque incluyan datos reales (email, página web) de alguna empresa, ésta no es la emisora, sino la víctima del engaño.

Leyendas urbanas. Alardes imaginativos, en ocasiones muy elaborados, que cuentan historias fantásticas, terroríficas o simplemente increíbles. Internet contribuye a que bulos clásicos del tipo 'Elvis vive' se diseminen rápidamente, y ha generado otros nuevos.

2. VIENDO EL TEMA MÁS A FONDO

Las cadenas son esos mensajes que nos reenvían de vez en cuando los amigos. Suelen venir de gente conocida.

Principalmente hay tres tipos de cadenas: cadenas de amistad, cadenas bien, hoax.

2.1. Cadenas de amistad

Son esos mensajes que llegan de vez en cuando en tono bondadoso en las que se habla de lo bonito que es el cielo, la luz, la obra de Dios, el amor y otras cosas. Al final se pide que se reenvíe a 10 amigos y ya.

2.2. Cadenas de bien

Son los mensajes por el bien de alguien. Libertad para Frensz, el niño que se muere, etc. Este tipo de cadenas son las más corrientes, pero la mayoría de las veces resultan ser falsas, estar caducadas (Frensz ya está libre y el niño que se muere ya está a salvo). Este tipo de cadenas es el más importante por las siguientes razones:

1. Las causas nobles movilizan a mucha gente

2. La mayoría de la gente no se molesta en comprobar la naturaleza de lo que está enviado. Lo reenvía sin más, y esto es un problema.

3. La gente que lo recibe lo reenvía sistemáticamente.

4. La gente que lo reenvía, inserta muchas direcciones de su libreta.

5. La gente que lo reenvía NO SE MOLESTA EN QUITAR LAS DIRECCIONES ANTERIORES. Aquí reside el gran problema, y la madre del cordero.

Si vas a participar en una causa noble, en la que se necesitan X personas que apoyen la causa, no olvides lo siguiente:

a) Un e-mail NO tiene validez legal. Es decir, que si te piden poner tu nombre al final de una lista, y que reenvíes el mensaje, eso no vale para nada. Si pones tu email, no librarás a nadie de la horca, ni te regalarán un móvil.

b) Si vas a interesarte por una de estas causas, interésate de verdad. No hagas únicamente lo que pone en el email y con eso pienses que ya has cumplido. Moléstate un poco, entra a Internet y comprueba en qué estado se encuentra dicha causa. En definitiva, comprueba que no es un bulo (hoax) y de no serlo, comprueba que realmente hay una campaña de sensibilización activa.

2.3. Cadenas de hoax

La mayoría de los mensajes que van dirigidos a más de 10 personas y te piden que hagas algo son hoax. Un hoax es un bulo, una leyenda urbana, un cuento, que corre de email en email. Su alta distribución se debe a que los usuarios adictos a los hoax no comprueban dicha información antes de reenviarla a sus muchos contactos, y tampoco se molestan en quitar las direcciones al reenviar los mensajes. Así que cada hoax, además de portar un cuento, porta decenas (a veces cientos) de emails (listas que irán a parar a manos de los spammers). A veces, los hoax están basados es un hecho real, o en una cadena del bien.

2.4. Hoax

Un hoax es un mensaje de contenido falso con dos objetivos principales: embaucar e incitar a su reenvío. Esas dos características ayudan a identificarlo y desdeñarlo: incluyen expresiones de alarma para llamar la atención y, bajo el pretexto de la solidaridad o la seguridad, apremian a que se comparta con el mayor número de personas posibles.

Ningún mensaje de alerta de una entidad digna de crédito solicitaría el reenvío del mensaje a todos los conocidos. Esto debería bastar para menospreciar el aviso, pero los hoax se las ingenian para engañar al receptor utilizando ardides más o menos sofisticados (ingeniería social), como el lenguaje técnico o el respaldo en alguna entidad de prestigio.

El contenido de los hoax es similar al de las cadenas de mensaje, y suelen incluir tres partes:

Gancho. Para captar el interés, tanto en el 'asunto' del mensaje como al principio del texto. Mediante frases como 'Alerta virus', 'Hazte rico en dos días' o 'Una niña necesita tu ayuda', apelan al miedo por un estropicio en la computadora o la compasión por alguien que necesita ayuda.

Amenaza. Advierte de las terribles consecuencias de romper la cadena. Los falsos avisos de virus confían más en que nadie dejará de avisar a sus conocidos de un peligro en ciernes.

Petición. En los esquemas piramidales se solicita enviar algo de dinero a varias personas para, en un futuro incierto, recibir una fuerte suma; la versión electrónica de este fraude simplemente solicita el reenvío masivo para compartir un aviso o tener suerte.

Hay otra serie de detalles que deben hacer sonar la señal de alarma en el receptor como los errores flagrantes en la redacción (fruto de las múltiples traducciones de la fuente original), la ausencia de fechas (para que el timo no caduque) y la inexistencia o falsedad de la información de contacto.

El usuario puede sospechar, de esta manera, que le intentan dar gato por liebre y optar por destruir el mensaje o cerciorarse de la falsedad del texto y contribuir a poner fin al engaño. Estos son algunos consejos:

Si el aviso se apoya en alguna fuente seria, no está de más consultar su página web para certificar la veracidad del mensaje.

Si la alerta hace referencia a algún supuesto virus alojado en el sistema, es fácil comprobar si el archivo en cuestión está presente en todas los PCs que comparten sistema operativo.

Tanto para los hoax (cadenas, leyendas urbanas, etc.) como para los virus siempre es muy útil comprobar los listados

facilitados por los fabricantes de antivirus (como la de McAfee o Panda Software) o por otras muchas páginas especializadas.

Por tanto, ante la presencia de un email sospechoso jamás se debe reenviar a nadie y menos remitirlo a toda la libreta de direcciones. Si se trata de una alerta sobre un virus auténtico, se puede distribuir evitando el tono alarmista e incluyendo información para la cura si es posible. Si se comprueba que es un bulo conviene responder al remitente, sin tono recriminatorio, explicando que se trata de una patraña y cómo debe actuar en el futuro ante este tipo de correos.

En cualquier caso, nunca se debe utilizar la opción de 'reenviar' en los mensajes sospechosos, puesto que si hay algún archivo adjunto maligno seguirá distribuyéndose y además se incluirán todas las direcciones de correo de los anteriores receptores. En caso de enviar el mensaje a varios destinatarios, conviene colocar las direcciones en el apartado 'CCO:' (copia oculta) para que los emails no terminen cayendo en manos extrañas.

2.5. Nuevos bulos

Nuevos bulos aparecen casi a diario en Internet. Además, son tan difíciles de detener, que algunos siguen dando la lata muchos años después de su creación. Las enciclopedias víricas contienen más de un centenar de variantes de hoax que contaminan la Red. Aquí hay algunos ejemplos: Listado de hoax:

2.1.1 Clásicos

Good Times, el primer hoax de extensión masiva, sigue en activo después de su 'lanzamiento'. Good Times creó escuela alertando sobre un ejecutable que llegaba por correo y, con sólo leer el mensaje, era capaz de destruir el disco duro y hasta el procesador.

Penpal Greetings es otro clásico, en activo desde que IBM (falso, por supuesto) envió la alerta en noviembre de 1997. Con al menos tres variantes, este hoax también auguraba terribles catástrofes informáticas al que recibiese el inexistente virus.

Bud Frogs screensaver. El salvapantallas de las ranas protagonistas de la publicidad de la cerveza Budweiser, cuya descarga eliminaría el contenido del disco duro, es un bulo de gran éxito. Aunque tenga más de cinco años de antigüedad, aparece nada menos que en el tercer puesto de los hoax más notables de enero de 2003 elaborado por Sohos.

2.5.2. Dañinos

JDBGMGR o Teddy, JDBMGR, JBDGMGR, Teddybear... está entre los falsos virus más extendidos actualmente. Apremia a eliminar el archivo jdbgmgr.exe de Windows para protegerse del virus Bugbear (auténtico), con lo que sólo se conseguirá que no se carguen de manera correcta algunas páginas web que utilicen applets de Java.

Sulfnbk.exe. Parecido al anterior, incita a eliminar el virus del mismo nombre y avisar a todas las personas. Si se le hace caso, los nombres de archivos largos se verán truncados a 8 caracteres.

2.5.3. Móviles

Virus on mobile phone. Hay varios hoax referentes a teléfonos móviles. Uno de los más extendidos dice: "Si recibe una llamada y en la pantalla del teléfono aparece "UNAVAILABLE!?", no responda, puesto que su móvil será infectado por un virus. La información ha sido confirmada por Motorola y Nokia y el virus ya ha infectado a 3 millones de móviles".

2.5.4. Leyendas Urbanas

Bill Gates comparte su fortuna. Puede parecer mentira, pero no lo es: un email que asegura que Microsoft pagará 245 dólares cada vez que sea reenviado se ha situado durante varios meses consecutivos entre las leyendas urbanas más distribuidas por Internet.

3. CONCLUSIONES

Hemos visto que lo que nos llega por email, no siempre es lo que parece. Ahora puedes creer que esta interpretación es muy negativa y bastante borde. Pero dejarás de pensarlo siempre y cuando seas víctima de esto. Así que aunque esto te pueda parecer alarmista, es justo ahora cuando todavía puedes hacer algo, y evitar caer en este tipo de engaños.

4. REFERENCIAS

[1]http://www.thehouseofblogs.com/articulo/que_es_un_ bulo_o_hoax-991.html

[2]http://wapedia.mobi/es/Hoax

[3]http://desenmascarandofraudes.blogspot.com/

[4]http://www.consumer.es/web/es/tecnologia/internet/2003/03/12/58907.php

[5]http://www.pclandia.net/articulos/hoax.htm

[6]http://www.rompecadenas.com.ar/hoaxes.htm

[7]http://es.wikipedia.org/wiki/Bulo#Bulo_inform.C3.A1 tico

[8]http://historiasdeblog.myblog.es/historiasdeblog/art/2138752/Bulos-Hoax-enganos-en-Internet

[9]http://quinn85.wordpress.com/2009/09/28/bulo-i nformatico/