

Combatiendo el correo basura: un enfoque inteligente del problema

Introducción

El correo basura (*spam*) es el peor enemigo del correo electrónico. Los estudios indican que, de todos los mensajes recibidos en los buzones electrónicos, un 90% es correo basura. Los emisores de este tipo de mensajes (*spammers*) ganan fortunas con este negocio, pero pocos países toman acciones legales contra los responsables.

Algunas personas creen que el correo basura no puede ser eliminado, y que hay que resignarse a padecer su existencia.

Sin embargo, pueden tomarse precauciones para minimizar sus efectos.

En este documento detallamos los peligros del correo basura, y las últimas técnicas utilizadas por sus emisores. También ofrecemos una serie de consejos prácticos, para reaccionar con inteligencia ante los mensajes no solicitados (sin la ayuda de aplicaciones especializadas en este problema), con el fin de mantener intactos sus datos y su privacidad.

Ejemplos de correo basura

Si bien no existe una definición exacta, se denomina correo basura a los mensajes de correo electrónico (o cualquier mensaje distribuido a través de un medio de comunicación digital, por ejemplo los mensajeros instantáneos) no solicitados, enviados sin la aprobación explícita del destinatario. Estos mensajes son distribuidos masivamente a millones de receptores, y sus autores buscan obtener una recompensa económica de los comerciantes cuyos bienes y servicios anuncian.

Medicamentos genéricos, réplicas de relojes, préstamos a bajo interés, y sitios de contenido para adultos encabezan la lista de favoritos de los emisores de correo basura.

Ejemplo 1

En este caso, el texto del mensaje está dentro de la imagen. De este modo, es más difícil que un filtro tradicional de correo no deseado pueda identificarlo como tal. Los textos que acompañan al gráfico utilizan vocabulario profesional, para aumentar la sensación de legitimidad.

From: Christopher L. Quinn
Date: Wednesday, February 15, 2006 4:50 PM
To: advertiser@...com
Cc: ...@...com; ...@...com
Subject: Invitation #4672

refection the coda in abrupt or townhouse not adopt or stylish or avis
a



Canadian Pharmacy, discreet, no prescription!
Viagra - Cialis - Xanax - Valium - Tamiflu
Get Xanax and Valium, NO PRESCRIPTION!

Ejemplo 2

Muestra el caso del “Fraude nigeriano” (*Nigerian Scam*), o fraude financiero (“401-spam”).

Generalmente, las cartas de este tipo simulan provenir de un soberano destronado, que ofrece enormes beneficios a cambio de una pequeña inversión para recuperar tesoros ocultos.

Este mensaje tan particular también esconde un virus en la imagen adjunta.



Greetings to you and Please permit me to introduce myself. I am Mr. ALSHEIKH RAHMAN a Saudi National and a crude oil Merchant befo according to medical experts I only have a few more months to live.

El fraude financiero se realiza mediante el envío de cartas que parecen auténticas, aparentemente provenientes de instituciones financieras confiables, y que intentan obtener las credenciales de las víctimas para sustraer los fondos de sus cuentas, o realizar otras transacciones ilegales en nombre del usuario autorizado.

Este tipo de fraude se conoce como falsificación de sitios (*phishing*), y es muy importante estar alerta ante esta amenaza, para prevenir el robo de identidad.

🔗 La falsificación de sitios ya ha sido detallada en un [artículo previo](#) de esta sección.

Los riesgos ocultos del correo no deseado

El envío de publicidad no solicitada, invitaciones y falsas ofertas para enriquecerse rápidamente, se denomina correo basura “seguro”, pues los mensajes sólo apuntan a vender determinados productos.

Pero, además de esta función básica, el correo no deseado puede ser realmente destructivo cuando utiliza código malicioso en un archivo adjunto o un hipervínculo.

Este tipo de mensaje masivo puede transportar una carga peligrosa, bajo la apariencia de un documento o fotografía inocente.

El individuo que lo envía, intenta persuadir al receptor para que abra dichos archivos, utilizando señuelos como “El video de Osama Bin Laden”, o “Imágenes exclusivas de la vida privada de David Beckham”.

Utilizando vulnerabilidades de la aplicación cliente de correo electrónico, como Microsoft Outlook u Outlook Express, el código malicioso puede ejecutarse por su cuenta, sin la participación ni el conocimiento del usuario.

Además de los peligros mencionados, al pulsar sobre un hipervínculo contenido en un correo basura, el usuario corre el riesgo de infectar su ordenador con troyanos o programas espía.

Estos programas maliciosos se descargan automáticamente aprovechando fallas de seguridad no reparadas del programa navegador.

Una buena medida para evitar que esto suceda es no abrir nunca archivos adjuntos, ni pulsar sobre los hipervínculos contenidos en mensajes provenientes de desconocidos.

Cómo consiguen las direcciones electrónicas los emisores de correo no deseado

Obviamente, para enviar un correo basura, los emisores del mensaje necesitan la dirección del receptor.

Existen varias formas para obtener estos datos, pero en la mayoría de los casos es el mismo usuario quien, inadvertidamente, provee su dirección de correo en sitios de dudosa reputación.

A continuación mencionamos una serie de precauciones para evitar que su dirección de correo electrónico se incluya en las bases de datos de los emisores de correo no deseado:

- Evite incluir su dirección electrónica personal en foros abiertos, cuadernos bitácora, o grupos de noticias. Si fuera obligatorio ingresar su información de contacto en estos sitios, intente retocarla un poco de modo que los robots buscadores de direcciones no puedan descifrarla fácilmente. Por ejemplo, si su dirección de correo es `juan@dominio.com`, podría publicar “Juan(arroba)dominio(punto){-com-}”. Un humano descubriría rápidamente la dirección real, pero un robot no podría traducirla con facilidad.
- No responda mensajes no deseados, ni pulse en los vínculos publicados en este tipo de correo. También es muy importante que nunca utilice la opción “dejar de recibir este correo”. Al hacerlo, está confirmando al emisor del mensaje, que su dirección de correo es válida.
- Desconfíe de cualquier mensaje proveniente de un amigo, que incluya un archivo adjunto no solicitado explícitamente con anterioridad. Este método se utiliza con frecuencia para diseminar un gusano en todos los contactos de su libreta de direcciones. En caso de duda, averigüe si, efectivamente, su amigo le ha enviado el archivo.

- Si recibe un mensaje que no está esperando, de alguien a quien no conoce, asuma que es correo basura.

- Utilice cuentas de correo distintas para propósitos diferentes.

Recuerde que los emisores de correo no deseado comercializan listas de direcciones.

Si mantiene en secreto los datos de su cuenta principal mientras está en línea, seguramente el riesgo de recibir correo basura en su buzón será mínimo.

Cómo se propaga el correo no deseado

Generalmente, los individuos que envían correo basura, no utilizan sus propios ordenadores para distribuir los mensajes: se valen de verdaderos ejércitos de ordenadores "esclavos", que realizan esa tarea.

Este conjunto de máquinas, conocido como *botnets* (ordenadores con acceso a Internet de alta velocidad, controlados por un programa de acceso remoto), es capaz de enviar millones de mensajes por día.

Los gusanos y los troyanos también pueden enviar una enorme cantidad de correo electrónico no deseado, pues se propagan rápidamente de un ordenador a otro a través de Internet durante su etapa de actividad.

Cómo proteger sus datos

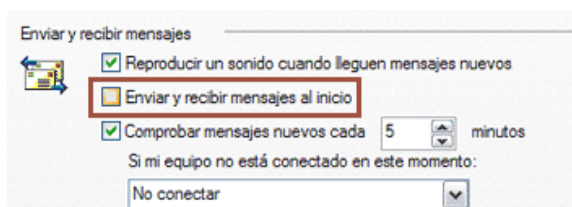
En principio, es importante que reconozca el correo basura y actúe en consecuencia.

La información contenida en este artículo lo ayudará a distinguir con mayor facilidad el correo no deseado, y a continuación encontrará una serie de consejos para reducir la cantidad de mensajes no solicitados que ingresan a su cuenta.

- Asegúrese de instalar Windows XP Service Pack 2, y las subsiguientes actualizaciones de Windows. De esta manera mantendrá el sistema operativo menos vulnerable ante esta amenaza.
- Instale una aplicación cortafuegos acreditada. Programas como Outpost Firewall Pro evitarán que su ordenador sea utilizado para enviar correo basura saliente a causa de una infección por código malicioso. El cortafuegos también puede configurarse para mantener en cuarentena los archivos adjuntos de un mensaje de correo electrónico, para que no puedan activar un posible troyano o virus al ser abiertos.
- Instale una aplicación antivirus que revise los archivos adjuntos del correo entrante y saliente en busca de virus.
- Verifique las medidas de seguridad que le brinda su servidor de correo electrónico. La mayoría de ellos ofrece herramientas de protección contra correo basura en su página principal. Estas herramientas pueden utilizarse para construir listas de direcciones que no desea admitir, y listas seguras con los contactos de personas conocidas. En algunos casos, también podrá configurar reglas para administrar el correo entrante de acuerdo a determinadas características.
- En lo posible, consiga una cuenta de correo de su proveedor de Internet (ISP) que permita la utilización de un protocolo de acceso a los mensajes almacenados en el servidor (IMAP, *Internet Message Access Protocol*). El protocolo IMAP permite descargar sólo los encabezados del correo entrante, de modo que al ver el remitente y el asunto de cada mensaje, rápidamente se puede identificar y eliminar el correo no deseado.
- Utilice programas de correo electrónico que tengan protección contra correo basura incorporada, como **Outlook** o **The Bat!**; y asegúrese de configurarlo apropiadamente. Si usa Outlook Express, realice las siguientes modificaciones, utilizando el menú Herramientas - **Opciones**:

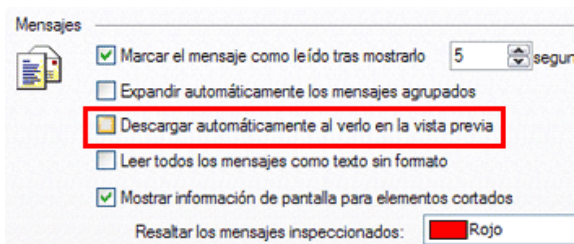
a) En la pestaña **General**, desactive la opción "Enviar y recibir mensajes al inicio".

b) Los otros parámetros son opcionales.

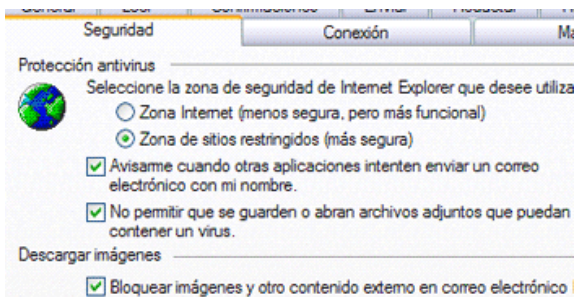


c) En la pestaña **Leer**, desactive la opción “Descargar automáticamente al verlo en la vista previa”.

d) Los otros parámetros son opcionales.



e) En la pestaña **Seguridad**, realice las modificaciones como muestra la figura.



Conclusión

En este artículo se han presentado algunos conceptos básicos contra el correo basura, que le permitirán controlar y administrar con inteligencia el correo no deseado que llega a su bandeja de entrada.

De este modo podrá limitar los peligros que ocasiona esta amenaza, aunque no logre eliminarla por completo.

En una próxima edición de **Conociendo más sobre seguridad informática**, analizaremos algunas aplicaciones especializadas contra el correo no deseado, para que pueda librarse de los mensajes no solicitados.

¡Le deseamos envíos de correo seguros!