Tutorial sobre Spam

Recopilado por SH-RooT

Teléfono y fax en Argentina: (5411) 4953 2061
Teléfono y fax en Costa Rica: (506) 253 5027
E-mail: info@codigosur.org
Web: www.codigosur.org

Código Sur

Tutorial sobre Spam
Por SH-RooT

© Código Sur - 2007

El trabajo de Código Sur ha nacido y se construye sobre la función democratizadora de la comunicación y su implicancia en la sociedad moderna, con la convicción de que permite accionar en favor de otro mundo posible, más participativo y con espacio para todos.

Reconociendo la importancia de socializar las herramientas de comunicación, Código Sur se ha especializado en brindar servicios de diseño gáfico y web, desarrollos y proyectos en Internet y TIC, prensa y difusión, realización audiovisual y comunicación institucional a las organizaciones de la sociedad civil de América Latina con el objetivo de colaborar con el desarrollo tecnológico y el acceso a la información.

Desde las sedes regionales de San José de Costa Rica y Buenos Aires Argentina, se llevan adelante proyectos y programas que apuntan a fomentar la comunicación en diferentes temáticas y áreas específicas.

http://www.codigosur.org

Índice

Qué es el Spam y por qué no queremos hacerlo

Se denomina Spam o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por Spam cualquier mensaje no solicitado.

El problema del Spam es tan grande que representa alrededor del 80% de todo el correo electrónico circulante en el mundo, según datos de varias fuentes (que ponemos a disposición en los contenidos del tutorial).

En el mundo existen algunos grupos que trabajan mancomunadamente con las autoridades gubernamentales y los ISP para perseguir a los spammers. La base de datos Register of Known Spam Operations (ROKSO) o en español Registro de Operaciones de Spam Conocidas, recoge información y evidencias electrónicas de operaciones de Spam que hayan reincidido al menos tres veces tras las notificaciones de los ISP, es decir que sólo hace falta que tres ISP hayan presentado denuncias, con su respectiva prueba, para aparecer listado ahí.

Según estudios, el 80% de los usuarios de internet considera muy molesto recibir Spam, además de que para hacerlo el usuario está pagando un servicio de Internet. Imaginemos que si solamente el 1% de los usuarios de internet enviara un Spam al día al resto de los usuarios, estaríamos recibiendo más de 1000 Spam por día. A esto se suma que el tráfico de centenares de miles de correos que se ejecuta de una sola vez congestiona el uso de los procesadores de las computadoras que prestan los servicios, con lo cual si continuara aumentando indefinidamente el tráfico del Spam, los proveedores tendrían que enfrentar inversiones que encarecerían ampliamente los costos de los servicios de internet .

Este tutorial sobre el Spam pretende reunir en un solo documento la información básica sobre este fenómeno que viene creciendo cada vez más y que tiene altos costos para proveedores, administradores y usuarios/as.

He realizado una selección de artículos y documentos encontrados por medio de Google, que creo puede complementar nuestro entendimiento y conocimiento general acerca del Spam. Cada artículo y documento reproducido tiene su aviso de copyrigth, su nombre y la URL correspondiente de donde fue extraído. El resto del documento (o sea lo que no es citado de sitios web),

está realizado bajo Licencia Creative Commons Argentina (ver página 2).

Es importante que las personas y organizaciones usuarias de los servidores de correo de Código Sur lean y entiendan este tutorial porque consideramos que hacer Spam es una práctica perjudicial para usuarios/as, administradores y proveedores, y todos somos responsables del uso que se haga de los servidores de Código Sur.

Esperamos que esta información les sea útil e interesante.

Hasta el próximo tutorial.

SH-RooT

URL's para visitar
Cretive Commons: http://www.creativecommons.org
Wikipedia: http://www.wikipedia.org
Código Sur: http://www.codigosur.org

El origen del término "Spam"

El origen de la palabra Spam es particularmente llamativo, ya que no son las siglas para denominar un tipo de protocolo cuyas letras siempre quieren decir algo (como GNU o HTML). Claro que son siglas, pero de algo que no tiene nada que ver con el mundo de la informática sino de la comida enlatada.

Aunque no lo crean, SPAM se llamó la primera carne enlatada del mundo que no necesitaba refrigeración. Su nombre completo era Spiced Ham que quiere decir Jamón con Especias, de ahí su nombre (Spiced Ham).

Esta carne ampliamente comercializada y distribuida aún en la actualidad en todo el mundo, fue durante la Segunda guerra mundial la comida por excelencia de las tropas de los británicos y los soviéticos, generando en la población una sensación de hastío relacionada con la marca SPAM y la carne enlatada.

El grupo cómico inglés Monty Python, burlándose de ese hartazgo de la comida enlatada, hace una parodia en la que todos los platos ofrecidos contenían SPAM y no era posible pedir un plato sin él.

En internet el primer uso del concepto Spam para denominar al correo basura surgió en grupos de noticias cuando un usuario envió un correo quejándose de todo el volumen de correo no solicitado que estaba recibiendo y hacía referencia al episodio de los Monty Phyton para describir la interferencia que eso generaba en la comunicación.

Así el término se fue difundiendo hasta popularizarse en todo el mundo y no es casual que varios lenguajes y productos en internet (como el lenguaje Python) deban su nombre al famoso y delirante grupo británico.

Según Wikipedia, *el Spam mediante el servicio de correo electrónico nace el 5 de marzo de 1994, cuando la firma de abogados Canter and Siegel publica en Usenet un mensaje publicitario. Al día siguiente, la firma facturó cerca de 10.000 dólares por casos de amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados.*

El nombre técnico del Spam es UBM o UBE por sus siglas en inglés (Unsolicited Bulk Mail / Unsolicited Bulk E-mail) que quiere decir: correos masivos iguales no solicitados. La imagen negativa del Spam está asociada principalmente a que las personas que lo practican a sabiendas o por ignorancia llegan al destinatario irrumpiendo en su privacidad y transfiriendo los costos a administradores y usuarios/as.

El Spam en internet es cualquier mensaje que sea enviado sin que lo soliciten, que se igual y que se distribuya en forma masiva. Esto incluye las pirámides, las advertencias de virus falsos, los anuncios de empresas con productos a la venta, listas y boletines electrónicos que suscriben correos sin autorización del usuario/a, etc.

URL's para visitar:
Definición de Spam en Wikipedia: http://es.wikipedia.org/wiki/Spam
Sketch Monty Phyton SPAM, subtitulado en español: http://www.youtube.com/watch?v=d7uFntkoBnk
Sketch Monty Phyton SPAM, doblado en español: http://www.youtube.com/watch?v=29LcVqeE96k
Empresa Hormel Foods (SPAM): http://www.spam.com

El Spam en números

Un informe de Monografías.com brinda algunos datos sobre el Spam a nivel estadístico.

El Spam representa más del 75% del tráfico total de correo electrónico *que circula en internet, hace tres años representaba sólo el 8%.*

14.5 ***billones de mensajes Spam son enviados cada día****, esto le representa a las empresas un costo de aproximadamente 20.5 millones de dólares por año globalmente.*

El Spam representa un riesgo para la seguridad y la privacidad*, debido a la proliferación excesiva de virus, esquemas "Phishing" y "robo de identidad".*

El 50% de los mensajes Spam provienen de computadoras zombis*, pues esto garantiza bajo costo, alta rentabilidad y adicionalmente anonimato para los spammers.*

9 ***de cada*** **10** *usuarios de Internet es afectado por el Spam.*

90% ***de los usuarios*** *de internet reciben correo basura.*

80% ***de los usuarios*** *de internet considera muy molesto el correo basura.*

Fuente: http://www.monografias.com/trabajos39/spam-correo-electronico/spam-correo-electronico.shtml

URL's para visitar:
Estadísticas del Spam en CAUCE (2004): http://www.cauce.org.ar/Estad%C3%ADsticasDelSpam
Diario El Comercio de Perú: http://www.elcomercio.com.pe/EdicionOnline/Html/2006-06-13/onlTecnologia0522314.html
Europa, segundo emisor de Spam: http://www.siliconnews.es/es/silicon/news/2007/07/19/europa-ya-es-principales

El Spam y el fraude electrónico

Hoy en día es común el uso de algunos términos para nombrar males asociados a la práctica del Spam. Palabras como phishing, spoofing, malware, crimeware, troyano, etc. llegan cada día a nuestros oídos y muchas veces no tenemos ni idea de que se está hablando.

La Wikipedia define al **phishing** como *un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas*.

Fuente: http://es.wikipedia.org/wiki/Phishing .

Siguiendo con las definiciones de Wikipedia, **spoofing**, *en términos de seguridad de redes, hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad*.

Fuente: http://es.wikipedia.org/wiki/Spoofing .

Malware *(del inglés malicious software, también llamado badware o software malicioso) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de softwares o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware*.

Fuente: http://es.wikipedia.org/wiki/Malware.

Posiblemente nos preguntaremos cómo es que operan estas personas y por qué motivo proliferan tanto los fraudes electrónicos por correo electrónico. El portal AméricaEconomía.com publica un artículo que nos cuenta la versión de Panda Software para entender cómo operan estas redes, los costos del malware y las ganancias que puede dar. Así lo describen:

Si dispone de US$ 1.200 en su bolsillo, tiene el principal requisito para transformarse en un ciberdelincuente y comenzar a obtener beneficios económicos de sus acciones maliciosas, según datos de PandaLabs, laboratorio de virus de Panda Software.

Para la compañía, esto es posible gracias al mercado negro que ha crecido en internet en torno al malware y que hace posible adquirir herramientas y códigos maliciosos a precios muy bajos.

Panda Software señala que si un ciberdelincuente quiere comprar un troyano, tendrá que pagar entre US$ 350 y US$ 700. Por ejemplo, un troyano password-stealer (ladrón de contraseñas) cuesta US$ 600, mientras que un troyano Limbo, que tiene menos funcionalidades, está en torno a los US$ 500, aunque puede encontrarse a un menor precio. Ambos están diseñados para el robo de contraseñas de acceso a bancos online. En cambio, si busca un troyano que capture cuentas de servicios de pago, como Webmoney, el ciber-delincuente debería desembolsar cómo máximo US$ 500.

Luego, el ciberdelincuente será dar con una serie de direcciones de correo a las que enviar el troyano. Para ello, le bastará con visitar otra de las páginas de este mercado del malware. En ella se ofrecen listados de cuentas de correo de todos los tamaños. Los precios oscilan entre los US$ 100 por el millón de direcciones y los US$ 1.500 por 32 millones.

El siguiente paso es asegurarse de que su código malicioso no lo va a detectar ningún antivirus. Por una cantidad de entre uno y cinco dólares, puede alquilar un servicio que protegerá su malware contra aquellas herramientas de seguridad que indique. Si el ciberdelincuente quiere hacerlo él mismo, puede hacerse con un software llamado Polaris por sólo US$ 20.

Luego, sólo queda enviar los correos electrónicos para distribuir el troyano. Para ello, puede alquilar un servidor exclusivamente para enviar spam. El precio está en torno a los US$ 500. Posteriormente, sólo debe aguardar por los resultados.

En resumen, para saber si el malware es rentable, basta con hacer unos sencillos cálculos. Si un troyano cuesta US$ 500 y una lista de correo de un millón de direcciones unos US$ 100, el gasto será de US$ 600 (Sólo con

este material, estará en disposición de infectar a un millón de personas). Se pueden sumar también a los gastos los US$ 20 que cuesta el programa de cifrado y US$ 500 por el servidor para enviar spam. Hasta aquí, la suma llega a US$ 1.100, más otros gastos varios de US$ 100 permiten una suma total de US$ 1.200.

Con un porcentaje de éxito de apenas un 10%, el hacker lograría colocar su troyano en el ordenador de 100.000 personas. Si de esa cifra, consigue robar datos bancarios a otro 10%, significaría que tiene a su disposición las cuentas bancarias de 10.000 personas. Basta imaginar el dinero que puede tener una persona normal en su banco y multiplicarlo por 10.000 para conseguir la cifra de beneficio del ciberdelincuente.

Ahora bien, vaciar un número tan alto de cuentas despertaría muchas sospechas y lo que todo delincuente persigue es hacerse con el dinero sin dejar huellas. Por ello, no cogerá todo el botín. Tan sólo sustraerá una pequeña cantidad de cada cuenta. ¿Ejemplo? Sólo US$ 100. Multiplicando esa cantidad por 10.000 obtenemos una cifra de un millón. Es decir, con apenas US$ 1.200 de inversión y en muy poco tiempo, uno de estos ciberdelincuentes puede hacerse millonario. Y esto, calculando con ratios de éxito realmente bajos. La realidad podría ser, aún, mucho peor.

Fuente: http://americaeconomia.com/PLT_WRITE-PAGE-SessionId--Language-0-Modality-0-Section-1-Content-31208-NamePage-IbizNoticiasArti-DateView--Style-15389.htm

URL's para visitar:

Discución del artículo en Foros Hack Hispano: http://www.hackhispano.com/foro/showthread.php?p=134707
Trucos psicológicos: http://riesgosinformaticos.com.ar/2007/07/16/internet-trucos-psicologicos-de-estafadores-para-robar-datos
Ingeniería Social: http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)

La redes spammers y los principales emisores

Los spammers buscan transferir el costo de sus operaciones a terceros, sean usuarios/as, sean administradores de sistema, sean ISP. En esto se basa su alta rentabilidad y claro está es lo que les permite que no puedan ser descubiertos.

En el mundo existen algunos grupos serios que intentan perseguir a los spammers y que trabajan mancomunadamente con las autoridades gubernamentales y los ISP. Una de las más destacadas internacionalmente en material de Spam es la organización Spamhaus. Ellos además de brindar soluciones para combatir el Spam han creado la base de datos ROKSO (por sus siglas en inglés) que identifica a los emisores de Spam, en muchos casos con nombre y apellido y las seudo compañías que permiten sus operaciones.

No es muy difícil ingresar en la base de datos ROKSO, sólo hace falta que tres ISP hayan presentado denuncias, con su respectiva prueba, para aparecer listado ahí. Al visitar la web de ROKSO uno comprende que Spamhaus no está jugando, ya que es posible encontrar los números de teléfono, nombres de empresas, nombres y apellidos de personas, cuentas de ICQ, cuentas de MSN, lugar de residencia y hasta ¡fotos de los spammers!

Un pequeño artículo del blog Todo es Electrónico nos cuenta lo siguiente:

La base de datos Register of Known Spam Operations (ROKSO) o en español Registro de Operaciones de Spam Conocidas, recoge información y evidencias electrónicas de operaciones de Spam profesionales que hayan reincidido al menos tres veces tras las notificaciones de los ISP.

Según este censo, 200 bandas son responsables del 80% del Spam recibido en Europa y América. La información se obtiene recopilando aliases, direcciones de email, dominios, redirecciones, ubicaciones de dominios y ordenadores anfitrión, que permiten llegar a un "núcleo duro" de 200 operaciones en las cuales intervienen 500-600 spammers profesionales que a su vez también van cambiando de dominios y apodos. Estos pájaros que operan ilegalmente se mueven de red en red y de país en país buscando ISP (Internet Service Providers, Proveedores de Servicios Internet) benignos a sus prácticas y que son conocidos por la laxitud de sus políticas "anti-spam".

La Base de Datos ROKSO de Spamhaus está disponible en una versión especial de acceso restringido a Cuerpos y Fuerzas de Seguridad (Law Enforcement Agencies) cualificadas que proporciona información sobre los registros de evidencias electrónicas, los logs (diarios electrónicos) y datos adicionales sobre las actividades ilegales de estas bandas que son demasiado sensibles como para ser expuestos de forma pública.

En el servicio de Spamhaus se recogen varios rankings interesantes. En la clasificación de países de los que procede el Spam destacan Estados Unidos, China y Japón. Los 10 *"peores" países desde el punto de vista del Spam son:*

Estados Unidos
China
Japón
Rusia
Canadá
Korea del Sur
Reino Unido
Taiwan
Hong Kong
Holanda

Fuente: http://inza.wordpress.com/2006/11/16/la-mayor-parte-del-spam-la-realizan-unas-pocas-bandas/

Según el informe 2006 de la empresa Sophos *Asia sigue siendo el continente que emite más Spam, no obstante, en Europa continúa creciendo el nivel de spam. En el primer trimestre de* 2006, *Europa era responsable del* 25% *del Spam, hoy alcanza el* 27,1%, *sobrepasando a América del Norte. La clasificación por continente entre abril y junio de* 2006 *es la siguiente:*
Abril a junio de 2006

1. *Asia:* 40.2%
2. *Europa:* 27.1%
3. *América del Norte:* 25.7%
4. *América del Sur:* 5.5%
5. *Oceanía:* 0.7%
6. *África:* 0.7%

Resulta raro comprobar la ausencia de Rusia entre los principales países emisores de Spam. Sin embargo, Sophos ha podido constatar que desde este país se controlan inmensas redes de ordenadores zombi con este propósito. Entre las pruebas, Sophos ha descubierto hace poco una lista de precios en ruso en el que ofrecen por 500 dólares hasta 11 millones de direcciones de email en Rusia. Por tan sólo 50 dólares se pueden adquirir 1 millón de direcciones de cualquier país.

Fuente: http://esp.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html

URL's para visitar:

Spam Haus: http://www.spamhaus.com
ROKSO: http://www.spamhaus.org/Rokso/
The 10 Worst ROKSO Spammers: http://www.spamhaus.org/statistics/spammers.lasso
The 10 Worst Spam Origin Countries: http://www.spamhaus.org/statistics/countries.lasso
Composite Blocking List: http://cbl.abuseat.org/
Coalition Against Unsolicited Commercial Email: http://www.cauce.org
Coalition Against Unsolicited Commercial Email Argentina: http://www.cauce.org.ar/
Coalición Europea Contra el Correo Comercial No Solicitado: www.euro.cauce.org/es/
AbuseNet: http://abuse.net/

Recomendaciones para recibir menos Spam

La Secetaría General de la Coordinación Administrativa de Tecnologías de Información de la Universidad de Yucatán, posee una sección de su sitio web dedicada al Spam. Esta página reúne muchos de los mejores consejos que hay en español en la web.

Consejos:

1) Intenta no hacer pública tu dirección de correo. Si tienes que publicar tu dirección de correo utiliza alguno de estos trucos:

Utiliza una dirección de e-mail temporal que puedes conseguir gratuitamente para publicarla en lugar de suministrar la dirección que utilices habitualmente.

Si luego tienes que prescindir de ella no afectará a tu buzón personal.

Sustituye el símbolo @ por la palabra ARROBA (en mayúsculas) al dar tu e-mail.

Añade el texto "QUITALASMAYUSCULAS" después de la arroba si es obligatorio el carácter @.

2) Lee y entiende la política de privacidad cuando suministres tu dirección de e-mail en un sitio web.

Mira si la política de privacidad permite a la compañía vender a terceras personas tu correo. Si esto fuera así, no envíes tu dirección de correo a estos sitios. Si no encuentras la Política de Privacidad, te parece sospechosa o no tienes claro quién es el responsable de una web, mejor que no les des tu e-mail.

3) Lee y comprende los formularios antes de transmitir información personal a través de la red.

Algunos sitios web permiten decirles que no quieres recibir correos suyos, pero seguramente tendrás que marcar alguna casilla para que esto se haga efectivo. En cualquier caso lee y entiende lo que te dicen antes de enviar la suscripción o el pedido.

4) Decide si te conviene utilizar más de una dirección de correo.

Una de ellas será para los mensajes más personales y la otra para usarla en las salas de chats o listas de distribución.

Esta última será una cuenta de correo desechable, es decir, si esta dirección empieza a recibir Correo Basura - Spam, puede cerrar esta cuenta y esto no afectará a tu correo personal o profesional.

5) Usa un nombre poco común en tus cuentas de e-mail.

La elección de tu dirección de correo puede afectar a la cantidad de Correo Basura - Spam que recibes.

Los Spammers seleccionan combinaciones de nombres posibles para un determinado proveedor de acceso a Internet, esperando encontrar direcciones válidas. Por esta razón, un nombre común como apmartin puede que tenga más cantidad de Correo Basura - Spam que ap50x25martin. El inconveniente es que optar una dirección inusual es más difícil de recordar.

6) Usa un filtro en tu correo.

Observa si tu gestor de correo (Eudora, Outlook, etc.) tiene alguna herramienta para filtrar los e-mails que contengan Correo Basura - Spam, para enviarlos directamente a alguna carpeta distinta a la de entrada de tus correos.

7) Combate y denuncia a los Spammers.

Si simplemente filtras el Correo Basura - Spam que recibes y no lo combates estarás contribuyendo a que sigan con sus prácticas.

8) Mantén tu superioridad moral frente al Spam.

No amenaces al spammer con violencia o vandalismo, no bombardees el sitio con mensajes, no bombardees al remitente con mensajes, puede tratarse de un tercero inocente, no ataques el sitio con métodos de piratería electrónica, técnicas de hacking, etc.; no intentes hacer caer el sitio por cualquier medio ilegal; y sobre todo, no recurras al envío de Correo Basura - Spam para luchar contra el Correo Basura - Spam.

9) Analiza las cabeceras para ver de dónde proviene.

Si crees que es un envío de alguien honesto envíale un correo para que te de de baja de su lista, si por el contrario sospechas que el emisor es un Spammer entonces lo mejor es localizar en las cabeceras el servidor desde donde se inició el envío y enviarle el comunicado a este servidor por si él puede hacer algo para evitarlo.

10*) Si el Correo Basura - Spam proviene u ofrece servicios de empresas, organismos o individuos españoles a los cuales no les has autorizado para que te envíen información a través del e-mail, envía copia al Ministerio de Ciencia y Tecnología y a la Agencia de Protección de datos.*

11*) Envía copia del Correo Basura - Spam a la sección de abusos de tu proveedor de e-mail, es decir de la empresa que gestiona tu buzón de correo electrónico. Si es un servidor privado o empresarial, entonces al Administrador del mismo.*

Normalmente la dirección suele ser: abuse@nombredetuisp.com o postmaster@nombredetuisp.com. Haciendo esto, permitirás dar a conocer a tu proveedor de acceso a Internet el problema con el Correo Basura - Spam que está llegando a tu buzón y ayudarás a atajarlo. Comprueba que la copia del Correo Basura - Spam incluye la cabecera del mensaje.

12*) Envía una queja al Proveedor de Servicio o ISP desde donde se realizo el envió masivo.*

La mayoría de los ISP quieren erradicar a los Spammers que saturan su sistema, para conocer el primer servidor de la red desde dónde se envió el Spam debes, necesariamente, de analizar las cabeceras y obtener este dato de aquí. De nuevo, asegúrate de remitir la cabecera del email junto con tu queja. En las cabeceras a veces solo aparece la dirección IP o el nombre de este servidor, utiliza las direcciones abuse@IP/nombredetuisp.com o postmaster@ IP/nombredetuisp.com para comunicarte con ellos.

13*) No respondas los mensajes no solicitados.*

Si respondes un mensaje no solicitado estarás confirmado que tu dirección está activa, con lo cual comenzarás a recibir aun más Spam.

Recomendaciones:

1- *Limita tus suscripciones a listas de correo de sitios desconocidos. Estos son pequeños formatos que dicen "Suscrí-*

bete para recibir un anuncio cuando actualicemos esta página". Muchas de estas páginas (principalmente las que tratan sobre estrategias de mercadotecnia y oportunidades de negocio en Internet) son un "gancho" y almacenan las direcciones de correo suministradas para luego venderlas a spammers (ver figura más abajo).

2- *Nunca suscribas tu página a programas como "Free For All (FFA)", que te proponen enviar tu sito a miles de buscadores. Estos "buscadores" son en realidad la página automática de ligas de una infinidad de sitios comerciales que utilizarán tu dirección para enviarte su publicidad y de la noche a la mañana saturan tu buzón con correo basura (y lo peor de todo es que en este caso no están faltando a la ley, porque TÚ los contactaste primero).*

3- *Nunca (repito: NUNCA) envíes dinero, el número de tu tarjeta de crédito o cualquier otra información personal a las direcciones incluidas en el mensaje. Es muy probable que se trate de un fraude.*

4- *No llames a los números telefónicos* 1-900 *que vienen en los mensajes. Frecuentemente se trata de números conectados a una grabación, que hacen un cargo por minuto a tu recibo telefónico.*

5- *No sigas los mensajes de cadena. Muchas personas actuando de buena fe, reenvían mensajes que reciben, como los que prometen dinero para ayudar a algún enfermo por cada reenvío del mensaje. Todos son falsos. No es posible rastrear todos los reenvíos de un e-mail. También son falsos los mensajes que prometen que Bill Gates o Microsoft van a pagar miles de dólares al que reenvíe un mensaje. Estos mensajes estrictamente hablando no son Spam, pero son una de las herramientas de los spammers.*

Desafortunadamente, después de algunos reenvíos, el mensaje en cadena contiene decenas y en ocasiones cientos de direcciones probadas de e-mail. Estas direcciones tarde o temprano llegan al buzón de un spammer y son coleccionadas para venderlas en grandes lotes a quienes las utilizan para enviar mensajes comerciales no solicitados.

Fuente: http://www.riuady.uady.mx/spam/

URL's para visitar:

Cómo combatir el Spam: http://cosassencillas.wordpress.com/2007/05/10/como-combatir-el-spam/

Diez consejos básicos para evitar el spam: http://noticiasdot.com/publicaciones/2003/0103/1701/noticias1701/noticias170103-13.htm

Servidores de correo de Código Sur

Código Sur opera sus servidores de correo con software que analiza tanto los mensajes entrantes como salientes para identificar aquellos correos que tienen virus o son Spam. Nuestro MTA (Mail Transfer Agent) es Postfix y nuestro MDA (Mail Delivery Agent) es Dovecot. Para procesar los mensajes, es el AMaViS quién se encarga de pasarle los correos al ClamAV o al SpamAssassin, antivirus y antispam respectivamente.

Postfix *es un Agente de Transporte de Correos (MTA) de código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail. Formalmente conocido como VMailer e IBM Secure Mailer, fue originalmente escrito por Wietse Venema durante su estancia en el Thomas J. Watson Research Center de IBM, y continúa siendo desarrollado activamente.*

Fuente: http://es.wikipedia.org/wiki/Postfix y http://www.postfix.org.

Dovecot *es un servidor de POP3 e IMAP (MDA) de fuente abierta que funciona en Linux y sistemas basados sobre Unix y está desarrollado con la seguridad como principal objetivo. Dovecot puede utilizar tanto el formato mbox como maildir y es compatible con las implementaciones de los servidores UW-IMAP y Courier IMAP.*

Fuente: http://www.dovecot.org y http://en.wikipedia.org/wiki/Dovecot_(software).

Amavis *se trata del establecimiento de un sistema antivirus para servidores de correo, concretamente para el servidor de SMTP, para monitorizar y/o detener correos portadores de virus y, opcionalmente, hacer lo mismo con el correo basura llamado Spam. En realidad, AMaViS no es realmente un antivirus, sino un servicio capaz de tomar el correo y suministrárselo a otro programa para su procesamiento. Cuando el servidor de correo recibe algún mensaje, se lo hace llegar al servidor de AMaViS, que, en función de como haya sido configurado, le pasara el mensaje a uno o varios programas antivirus, que habrán de adquirirse independientemente, y opcionalmente a programas detectores de Spam.*

Fuente: http://interno.ehas.org/intranet/organizacion/administracion-de-sistemas/AMaViS.

Clam AntiVirus *es un conjunto de herramientas GPL anti-virus para UNIX. El principal objetivo de este software es la integración con servidores de correo (analisis de adjuntos). El paquete dispone de un demonio*

multi-hilo flexible y escalable, un escaner de línea de comando, y una herramienta para actualización automática a través de Internet. Los programas se basan en una librería compartida distribuida con el paquete de Clam AntiVirus, que puede utilizar con su software. Aún más importante, la base de datos de virus se mantiene actualizada.

Fuente: http://www.clamav.net/about.

***Spamassassin** es una herramienta para inspeccionar correos electrónicos que permite determinar si se trata de un mensaje chatarra, mejor conocido como Spam. En este sentido Spamassasin es considerado un pre-procesador de correos, ya que la inspección es llevada acabo en el servidor de correos previo a que el usuario descargue su correo, así permitiendo una pre-clasificación de mensajes antes de utilizar una herramienta en PC (Outlook, Eudora o Mozilla).*

Fuente: http://www.osmosislatina.com/spamvirus/basico.htm.

URL's para visitar:
Postfix: http://www.postfix.org
Dovecot: http://www.dovecot.org
Amavis: http://www.amavis.org
ClamAV: http://www.clamav.net
Spamassassin: http://spamassassin.apache.org
Glosario de términos (1): https://www.agpd.es/index.php?idSeccion=541
Glosario de términos (2): http://www.uco.es/ccc/glosario/glosario.html
Glosario de términos (3): http://www.redcyt.secyt.gov.ar/glosario.htm

Políticas AntiSpam de Código Sur

Las políticas de Código Sur frente al Spam son muy rígidas. Está absolutamente prohibida, para cualquier persona usuaria de una cuenta personal o de una cuenta de eBoletines, la distribución de correo masivo no solicitado.

El incumplimiento de esta norma no sólo afectará su cuenta, ocasionando la cancelación de la misma de manera inmediata e irrevocable, sino que además pondrá en riesgo a toda la comunidad de sitios que se alojan en los servidores de Código Sur debiendo responsabilizarse la organización contratante de todos los daños económicos y judiciales que esto pudiera ocasionar.

El servicio de eBoletines es para el envío de boletines electrónicos con información generada por organizaciones y movimientos sociales para audiencias específicas. Si alguna persona considera que su privacidad ha sido violada por un administrador de una lista de eBoletines debe escribir inmediatamente a abuse@codigosur.org con la copia del correo en cuestión.

A la segunda queja de parte de un/a usuario/a o ISP sobre el envío de Spam la cuenta denunciada será suspendida sin derecho a reintegro.

El servicio eBoletines prohíbe la suscripción masiva desde el backend para administradores. Las únicas vías de suscripción son por medio del sitio web desde el recuadro de suscripción al boletín y mediante invitación que el administrador puede hacer desde el backend, debiendo el destinatario confirmar su suscripción.