UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

INVESTIGACIÓN DE MÉTODOS Y TÉCNICAS PARA COMBATIR EL SPAM.

Estudiante

Alexandra León Rodas

Tutor

Ing. Marco Lituma

Cuenca - Ecuador

2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Marco Lituma, certifico que la señorita Alexandra Patricia León Rodas con cédula de identidad 010559530-0 realizó la presente Tesis con el título **"INVESTIGACIÓN DE MÉTODOS Y TÉCNICAS PARA COMBATIR EL SPAM",** y que es autora intelectual del mismo, que es original auténtico y personal.

_____

Ing. Marco Lituma

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Tecnológica Israel, según lo establecido por la ley de propiedad intelectual, por su reglamento y por la normativa vigente.

_____

Alexandra Patricia León Rodas

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORIA

El documento de tesis con título **"INVESTIGACIÓN DE MÉTODOS Y TÉCNICAS PARA COMBATIR EL SPAM",** ha sido desarrollado por Alexandra Patricia León Rodas con cédula de identidad 010559530-0 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Alexandra Patricia León Rodas

DEDICATORIA

Este trabajo quiero dedicar especialmente a mis queridos padres Marcelo y Lourdes por todo el apoyo y comprensión que me han brindado para la culminación de esta tesis. A mis hermanos por el apoyo moral que me ofrecieron. Y de manera muy especial a mi querido abuelito que desde el cielo me dio muchas fuerzas para poder culminar este objetivo.

AGRADECIMIENTO

Agradezco al Ing. Marco Lituma, mi tutor por su eficaz cooperación y dedicación en esta labor, cuyo interés y constancia han hecho cumplir este objetivo

RESUMEN

El spam es correo electrónico no solicitado que llega a los buzones de manera arbitraria con el objetivo de vender o publicitar algo. Generalmente los productos y sitios que hacen uso de esta detestable práctica son de índole ilegal o fraudulenta

Además, el spam a menudo contiene material ofensivo y es posible que exponga al destinatario a fraudes. El spam también puede consumir servidores de correo electrónico e impacta de forma negativa en el rendimiento de la red.

Las consecuencias nefastas del "spam" surgen cuando los buzones de correo electrónico están repletos con decenas o cientos de mensajes publicitarios, perdiéndose mensajes auténticos en un mar de correos inservibles. En ocasiones existen buzones que son tan atacados por el "spam" que de cada 100 correos recibidos 99 de estos son correo no solicitado.

Es por eso que surge la iniciativa de realizar este proyecto de investigación ya que es un tema de este tema que está en constante evolución por la misma velocidad con la que crece el desarrollo en la tecnología y por la forma tan marcada en que se evidencia el impacto negativo de este fenómeno.

SUMARY

Spam is unsolicited email that reaches the arbitrary mailboxes in order to sell or advertise something. Generally the sites and products that make use of this abhorrent practice is illegal or fraudulent nature.

In addition, spam often contains offensive material and may expose the recipient to fraud. Spam can also take e-mail servers and impacts negatively on the performance of the network.

The harmful effects of "spam" arise when mailboxes are filled with tens or hundreds of advertising messages, messages lost in a sea of real junk mail. Sometimes there are so attacked mailboxes for "spam" that of every 100 emails received 99 of these are spam.

That arises is why the initiative for this research project because it is a subject of this issue that is constantly evolving with the same speed as the development grows and the technology so marked in evidence that the negative impact of this phenomenon.

Contenido

LISTADO DE CUADROS Y GRÁFICOS

LISTA DE ANEXOS

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

El spam es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del tráfico de correo electrónico total. Además, a medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el spam, los spammers (usuarios maliciosos que se dedican profesionalmente a enviar spam) se vuelven a su vez más sofisticados, y modifican sus técnicas con objeto de evitar las contramedidas desplegadas por los usuarios.

Ante el creciente aumento del spam y con ello un aumento de su impacto económico y la necesidad de combatirlo de una manera global, han surgido diferentes iniciativas que abordan el problema desde su raíz, la autenticación del remitente. Y es que la principal limitación por la que es tan sencillo enviar spam, es que cuando se diseñó el protocolo encargado de la transferencia de correos en 1.982 no se contempló la autenticación del emisor del mensaje, lo que facilita en gran medida la falsificación de direcciones en el envío de correo electrónico, característica que es aprovechada para fines maliciosos al permitir ocultar el remitente real o utilizar una dirección que al cliente le resulte familiar o confiable.

1.2 DIAGNOSTICO O PLANTEAMIENTO DE LA PROBLEMÁTICA GENERAL

1.2.1 CAUSAS Y EFECTOS

- El usuario pierde tiempo y dinero al descargar mensajes que no solicitó.
- Es molestado permanentemente con publicidad de cosas que no le interesan.
- Puede llegar un momento en que reciba más Spam que mensajes que realmente le interesan.

EFECTOS

- Inunda los buzones de correo, saturando la capacidad máxima de los mismos y por lo tanto, provocando la pérdida de correo deseado y útil.

- Afecta el tiempo empleado por los usuarios en leer, borrar, denunciar, filtrar etc.
- Amenaza la viabilidad del Internet como un medio efectivo de comunicación, comercio electrónico y productividad para las empresas.

1.2.2 PRONÓSTICO Y CONTROL DEL PRONÓSTICO

PRONÓSTICO:

Las empresas también tienen que realizar inversión en aumentar y mejorar el servidor de correo con el que cuentan para que pueda dar servicio al aumento de correo. Los usuarios tienen que hacer inversión en buscar, comprar e instalar filtros o programas antispam**,** para facilitar el trabajo a todos los trabajadores y garantizar la disminución sustancial del correo basura.

CONTROL DEL PRONÓSTICO:

En principio se puede pensar que esto no implica invertir mucho tiempo, pero si lo miramos desde el punto de vista que muchos trabajadores reciben gran cantidad de correo al día y éste se ve multiplicado por el spam, nos damos cuenta que lo más seguro es que se pase mucho más tiempo borrando correo no deseado que contestando a otros que si son importantes y que tienen que ver directamente con el negocio.

1.3 FORMULACION DE LA PROBLEMATICA ESPECÍFICA

1.3.1 PROBLEMA PRINCIPAL

La mayoria de usuarios del correo electrónico desconoce el daño que provoca el spam o correo no deseado como la propagación de virus informaticos, la pérdida de tiempo en leer, la identificación del e-mail como spam y borrarlo del buzón, con esto se intenta inducir el usuario a visitar páginas clonadas de instituciones financieras o a instalar programas maliciosos diseñados para hurtar datos personales y financieros

1.3.2 PROBLEMAS SECUNDARIOS

¿Cómo funciona?

¿Cómo se distribuye?

¿Quién los realiza?

¿Cómo obtiene el spammer mi dirección de correo?

¿Se utiliza algún tipo de software para controlar los mensajes Spam en una computadora?

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

- Identificar y estudiar 3 herramientas para combatir spam.

1.4.2 OBJETIVOS ESPECIFICOS

- Buscar las técnicas de envio de spam que se han desarrollado.
- Identificar el mecanismo de ataque que utilizan los spammers.
- Identificar los métodos para combatir el spam.
- Desarrollar la comparacion técnica y económica de las heramientas antispam estudiadas.
- Determinar cuáles son las consecuencias más significativas que surgen a raíz del problema y que impactan negativamente tanto a las empresas como usuarios comunes y corrientes.
- Generar recomendaciones y sugerir buenas prácticas para evitar en la medida de lo posible ser víctimas del spam y enfrentar el problema.

1.5 JUSTIFICACION

1.5.1 JUSTIFICACIÓN TEÓRICA

La Investigación busca presentar diferentes tipos de técnicas y métodos que ayudaran a contrarrestar el envió de spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido. Se pretende apoyar a los usuarios que son afectados con este tipo de correos, presentando una guía fundamental a la hora de escoger las mejores herramientas para combatir el spam.

1.5.2 JUSTIFICACIÓN METODOLÓGICA

Para la realización de esta investigación, se aplicara la metodología de investigación de campos, con la técnica de las encuestas a las personas que se sientan afectadas con este tipo correos no deseados con lo cual se conocerá los problemas que causan este tipo de mensajes, y así se podrá tener un mayor conocimiento de lo que causa el spam. Además se aplicara la técnica de la observación directa de la recepción de estos mensajes no deseados. Gracias a esto se tendrá datos reales y confiables.

1.5.3 JUSTIFICACIÓN PRÁCTICA

Con esta investigación se pretende dar una guía con la cual se podrá combatir este fenómeno que afecta a la mayoría de persona a nivel mundial, para que se tome las debidas precauciones y evitar todos aquellos comportamientos que faciliten la captura de las direcciones de correo electrónico.

CAPÍTULO II

MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

2.1.1 INTRODUCCIÓN

El uso del correo electrónico como medio de comunicación y transmisión de información va en aumento debido a su eficiencia y facilidad de uso. Desafortunadamente, por estas mismas características es utilizado para enviar correos masivos no solicitados (SPAM). Los índices de correo SPAM van en aumento, y por ello son necesarias técnicas y métodos para abatir este problema.

En todo este ambiente del servicio de correo electrónico se ha observado la presencia de correo masivo no solicitado, denominado correo SPAM. El SPAM contiene publicidad, invitaciones de visitas a otros sitios Web, entre otros contenidos. También pueden contener archivos con virus o programas pasivos, estos últimos usados para observar el contenido de nuestra computadora.

2.1.2 SPAM

El Spam o Correo electrónico no solicitado puede definirse como e-mails no deseados, habitualmente de tipo publicitario, que se envían aleatoriamente en grandes cantidades de usuarios. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

Se conoce como SPAM a la práctica de enviar correo no solicitado de forma indiscriminada, generalmente se trata de publicidad de productos o servicios. La acción de enviar este tipo de correos electrónicos se conoce como spamming, nace el 5 de marzo de 1994 cuando una firma de abogados Canter y Siegel, hacen un anuncio de su firma legal se publico en USENET[1] con lo cual en ese entonces logró facturar 10.000 dólares debido a la cantidad de lectores que existieron. También se llama correo no deseado a los mensajes sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes, drogas, software y

[1] USENET, Users Network, consiste en un sistema global de discusión en internet, donde los usuarios pueden leer o enviar mensajes sobre distintos grupos de noticias organizados de forma jerárquica.

pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas.

La cantidad de usuarios que recibe correo SPAM regularmente es de poco más de 78% y tardan un promedio de cinco minutos en borrarlos. Por otro lado, las empresas alrededor del mundo gastaron poco más de 20 mil millones de dólares en el año 2009 para contrarrestar el SPAM, además de la pérdida de productividad.[2] Usualmente la mayoría de las direcciones de correo utilizadas para enviar este tipo de correo son falsas, para ello una de las soluciones es que el remitente firme sus mensajes mediante criptografía de clave pública o certificados digitales.

El spam conlleva:

- Pérdida de tiempo. La información que no es de interés o utilidad para el usuario y tiene que eliminarla.
- Puede hacer perder información valiosa. Algunos correos válidos son clasificados como spam por algunos filtros, lo que hace que se pierda información útil e incluso vital.

El spam también se usa para enviar diferentes tipos de virus o intentos de estafa (phising).

2.1.3 SPAMMING

El spamming es el abuso de cualquier tipo de sistema de mensajes electrónicos y, por extensión, cualquier forma de abuso en otros medios como spam en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes en teléfonos móviles, etc. El spamming generalmente es originado por el ánimo de lucro de los spammers.[3] (Valenti; 2008).

2.1.4 SPAMMERS

Persona o grupo dedicados a la distribución de correo electrónico no deseado, o spam para promover productos o servicios. La actividad suele resultarles sumamente lucrativa, pero

[2] http://www.elpais.com/articulo/semana/combatir/spam/elpeputeccib/20070510elpciblse_4/Tes

[3] Valenti; Spamming, una práctica que afecta a la comunidad de Internet; http://www.isoc.org.ar/prensa/spamming.html; 2008.

está muy mal vista por la mayoría de los usuarios y empresas de internet, de hecho es ilegal en muchos países.

Los spammers son personas o empresas, que realizan el spam, obteniendo con esto una forma de publicidad muy rentable, ya que con un simple click se logra hacer llegar productos a millones de usuarios.

2.1.5 FORMAS DE SPAM

- **Correo electrónico:** Debido a la facilidad, rapidez y capacidad en las transmisiones de datos, la recepción de comunicaciones comerciales a través de este servicio de la sociedad de la información es la más usual, y el medio por el que los spammers envían más publicidad no deseada.

- **Spam por ventanas emergentes:** Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a Internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows titulado "servicio de visualización de los mensajes". Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario.

- **Hoax:** El hoax es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte. Los objetivos que persigue quien inicia un hoax son normalmente captar direcciones de correo o saturar la red o los servidores de correo.

- **Scam:** El Scam no tiene carácter de comunicación comercial. Este tipo de comunicación no deseada implica un fraude por medios telemáticos, bien vía teléfono móvil o por correo electrónico.

- **Spam en el móvil:** Además de las comunicaciones del operador de telefonía mediante mensajes de texto (SMS- Short Message Services), o mensajes

multimedia (MMS- Multimedia Message Services), existen otro tipo de comunicaciones publicitarias en las que no media un consentimiento previo ni una relación contractual, por lo que son consideradas comunicaciones comerciales no solicitadas.

Este tipo de comunicaciones generan un gasto de tiempo y de dinero. Además los MMS pueden introducir virus y explotar de forma maliciosa alguna vulnerabilidad de los sistemas internos del teléfono.[4]

2.1.6 FUNCIONAMIENTO DEL SPAM

Los spammers usan programas y tecnologías especiales para generar y transmitir los millones de mensajes de spam que son enviados cada día. Esto requiere significantes inversiones de tiempo y dinero.

Los spammers tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios. Con este objeto, utilizan distintas técnicas, algunas de ellas altamente sofisticadas.

2.1.7 CONTENIDO DEL SPAM

Se han encontrado innumerables mensajes basura, con gran diversidad de factores que los caracterizan y los categorizan como correo spam en las redes de comunicaciones y en nuestros buzones, y se ha logrado identificar un conjunto de características y contenidos que son comunes en este tipo de mensajes. A continuación se muestran algunos de los temas más comunes que vienen en el contenido de estos mensajes:

- Información sobre negocios piramidales para conseguir dinero de forma supuestamente fácil y rápida.

[4] http://www.zonavirus.com/articulos/formas-del-spam.asp

- Cadenas de cartas y mensajes del tipo, reenvía esta carta a 10 personas y tendrás una vida mejor.
- Enlaces a páginas Web pornográficas o líneas eróticas.
- Remedios milagrosos de cualquier tipo.
- Personas, generalmente niños (que son los que mas fácil nos conmueven el corazón) muy enfermos, los cuales podemos salvar enviando el correo que nos llega con la información a todos nuestros contactos y conocidos.

Todo lo anterior es clasificado como spam, es decir correo basura, correo que no hemos solicitado en ningún momento y que la persona que lo envía no tiene "permiso" ni autorización y/o consentimiento para enviarnos esta información. Lo que finalmente buscan con esto, es que el reenviar el mensaje una y otra vez, se recopilen gran cantidad de direcciones electrónicas de nuestros contactos y así también, las de los contactos de nuestros contactos. [5]

2.1.8 MÉTODOS DE DISTRIBUCIÓN DE SPAM

Existen diversas variantes, cada cual con su propio nombre asociado en función de su canal de distribución como son vía correo electrónico, en aplicaciones de mensajería instantánea (msn menssenger, yahoo messenger), en redes sociales, mediante dispositivos móviles a través de mensajes de texto.

2.1.9 PROBLEMAS QUE CAUSAN EL SPAM

El principal problema del Spam, es la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, así como de otros problemas que afectan a la seguridad y veracidad de este medio de comunicación: los virus informáticos, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre, el phising,

[5] http://www.clubplaneta.com.mx/correo/alerta_con_el_spam.htm

que son correos fraudulentos que intentan conseguir información bancaria. Los engaños que difunden noticias falsas masivamente o las cadenas de correo electrónico que consisten en reenviar un mensaje a mucha gente o la publicación de listas de direcciones de correo.[6]

Pérdida de productividad, Consumo de recursos de las redes corporativas: ancho de banda, espacio de disco, saturación del correo, etc. Algunos mensajes válidos importantes pueden ser borrados por error cuando eliminamos spam de forma rápida.

En un correo de spam se puede incluir muy fácilmente un archivo adjunto que contenga un virus, o un enlace a un sitio supuestamente interesante, desde el que se descargue algún tipo de código malicioso de forma oculta a los ojos del usuario. Llegando al extremo, incluso pueden llegar a ocultarse virus en el propio código del mensaje.

2.1.10 MEDIDAS PARA EVITAR EL SPAM

Como medida básica a adoptar para prevenir la entrada de spam en los buzones de correo de los usuarios, se encuentra el filtrado de mensajes de correo electrónico. Para ello existen un gran número de aplicaciones con las que pueden filtrarse correos electrónico por asunto, palabras clave, dominios, direcciones IP de las que provienen los mensajes, etc.

En el caso de empresas, el problema no reside únicamente en identificar correctamente los mensajes de spam, sino en gestionar adecuadamente las grandes cantidades de mensajes de este tipo que se reciben diariamente.

2.2 MARCO ESPACIAL

La determinacion de este estudio estara enfocado a todo el mundo ya que todos somos víctimas de este tipo de correos no deseados, con la finalidad de que la misma consiga todos los beneficios expuestas en la investigacion.

[6] Centro de alerta temprana sobre virus y seguridad informática; Anti-Spam. http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=11, 2005.

2.3 MARCO TEMPORAL

Para la investigación de métodos y técnicas para combatir el Spam, se contemplará un tiempo aproximado de 2 meses para su desarrollo, con lo cual se debera cumplir todas las actividades planteadas en el cronograma.

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1 UNIDAD DE ANÁLISIS

La investigación apoyará a todos los usuarios a la hora de escoger una técnica o un método con el cual se podra eliminar o combatir el spam.

3.2 TIPO DE INVESTIGACIÓN

La investigación contendrá varias características para alcanzar los objetivos planteados:

- Tipo exploratoria que permitirá investigar el mercado e ir descubriendo la realidad sorbe la problemática planteada. Además permitirá conseguir nueva información que enriquezca a la investigación de las nuevas tecnologías.

3.3 MÉTODO

Se hará uso de la metodología investigativa la misma que permitirá realizar una recopilación sistemática de la bibliografía, tecnología y estrategias necesaria para estructurar de forma adecuada la recopilación de la información.

3.4 TÉCNICAS E INSTRUMENTOS

Las técnicas e instrumentos de investigación para la recolección de la información que se utilizaron son los siguientes:

- Se aplicarán también los cuestionarios de encuesta que serán estructurados según las necesidades que presente la investigación, y serán aplicados a un conjunto preseleccionado de usuarios, estos cuestionarios servirán de base para la elaboración de las tablas estadísticas que sustentaron la presente investigación.

UNIVERSIDAD TECNOLÓGICA ISRAEL

Fecha.....

ENCUESTA:

Por favor complete la encuesta cuidadosamente al leerla por completo primero, y luego señale sus respuestas con una "x".

1. **¿Sabe usted que es el Spam?** (Marque con una X)

   Si ☐

   No ☐

2. **¿Usted ha sido víctima de Spam?**

   Si ☐

   No ☐

3. **¿Conoce usted las formas en que se distribuye el Spam?**

   Si ☐

   No ☐

4. **¿Qué clase de spam es el que mas les molesta?**

   Salud ☐ Tecnologías informáticas ☐ Entrenamiento ☐

   Pornografía ☐ Finanzas ☐ Educación ☐

5. **¿Conoce usted alguna herramienta para combatir el Spam?**

   Si ☐

   No ☐

6. **¿Sabe usted como obtiene el spammer (spammeador) su dirección de correo?**

   Si ☐

   No ☐

7. **¿Conoce usted las consecuencias de recibir Spam?**

   Si ☐

   No ☐

8. **¿Sabe usted como protegerse para no ser víctima del Spam?**

   Si ☐

   No ☐

Gracias por su colaboración, su aporte servirá de mucho.

JUSTIFICACIÓN DE LA ENCUESTA

1. **¿Sabe usted que es el Spam?**

   Se formúla esta pregunta con el fin de conocer si los encuestados tienen conocimiento del tema central que es el Spam.

2. **¿Usted ha sido víctima de Spam?**

   El fin de esta pregunta es saber si los encuentados han sido víctima de los envíos masivos de Spam.

3. **¿Conoce usted las formas en que se distribuye el Spam?**

   Se formúla esta pregunta para conocer si los encuestados saben como se distribuye el Spam y como llega a nuestras cuentas de correo de electrónico.

4. **¿Qué clase de spam es el que más le molesta?**

   Con esta pregunta se observará que tipo de Spam es el que más molestias causa a los usuario de correo electrónico.

5. **¿Conoce usted alguna herramienta para combatir el Spam?**
   Se formula esta pregunta con el fin de conocer si los usuarios de correo electrónico tienen conocimiento de alguna herramienta que les ayuda a eliminar el Spam.

6. **¿Sabe usted como obtiene el spammer (spammeador) su dirección de correo?**
   Con esta pregunta se conocerá si los encuestados saben como obtienen su dirección de correo los spammers para enviarnos el Spam.

7. **¿Conoce usted las consecuencias de recibir Spam?**
   Se formula esta pregunta para conocer si los usuarios de correo electrónico saben las consecuencias de recibir spam.
8. **¿Sabe usted como protegerse para no ser víctima del Spam?**
   Con esta pregunta se conocerá si los encuestados saben como protegerse para no recibir este tipo de correo no deseado.

MUESTREO

1. ¿Sabe usted que es el Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	19	95 %
NO	1	5 %
TOTAL	**20**	**100 %**

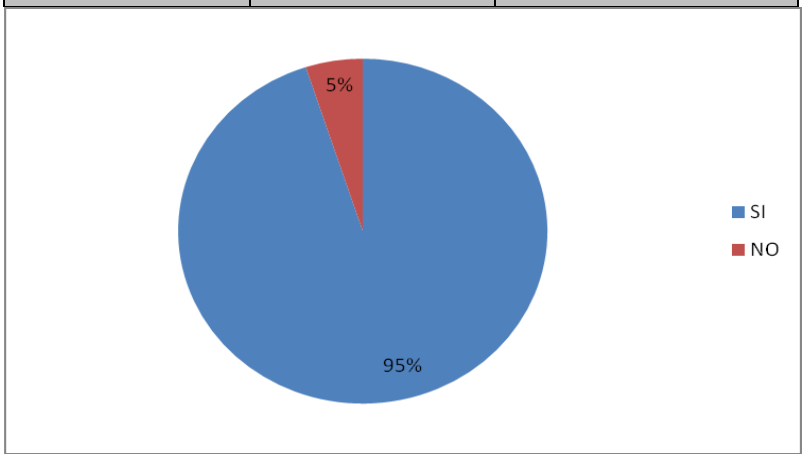


Ilustración 1: Resultado de la encuesta, pregunta # 1

Como se puede observar en el grafico el 95% de las personas encuestadas tienen conocimiento de lo que es un Spam.

2. ¿Usted ha sido víctima de Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	19	95 %
NO	1	5 %
TOTAL	**20**	**100 %**

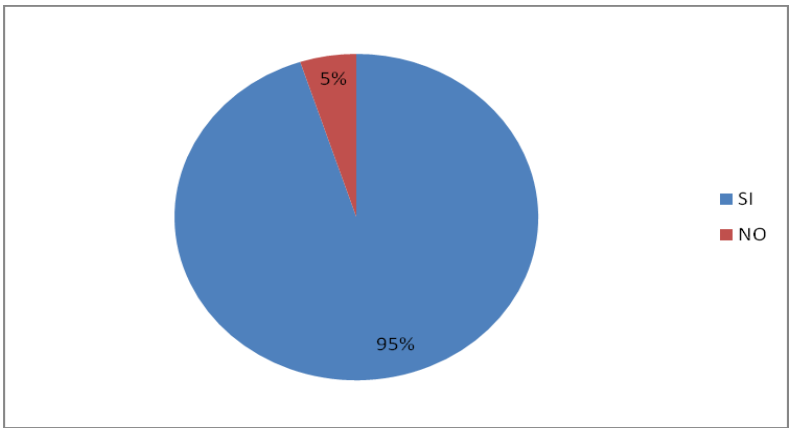


Ilustración 2: Resultado de la encuesta, pregunta # 2

El 95% de las personas encuestadas han sido víctimas de los envios masivos de Spam.

3. ¿Conoce usted las formas en que se distribuye el Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	4	20 %
NO	16	80 %
TOTAL	**20**	**100 %**

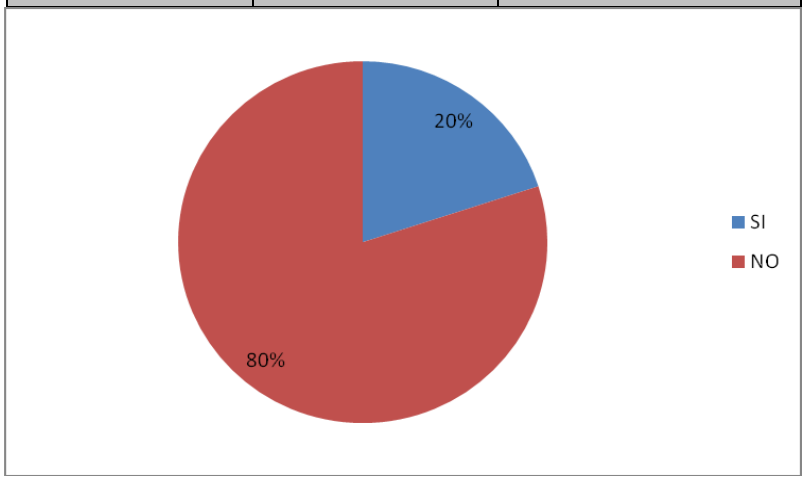


Ilustración 3: Resultado de la encuesta, pregunta # 3

El 80% de las personas encuestadas no tienen conocimiento como se distribuye el Spam y como llega a sus cuentas de correo electrónico.

4. ¿Qué clase de spam es el que más le molesta?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
Salud	4	20 %
Pornografía	12	60 %
Tecnologias Informáticas	1	5 %
Finanzas	1	5 %
Entretenimiento	1	5 %
Educación	1	5 %
TOTAL	**20**	**100 %**

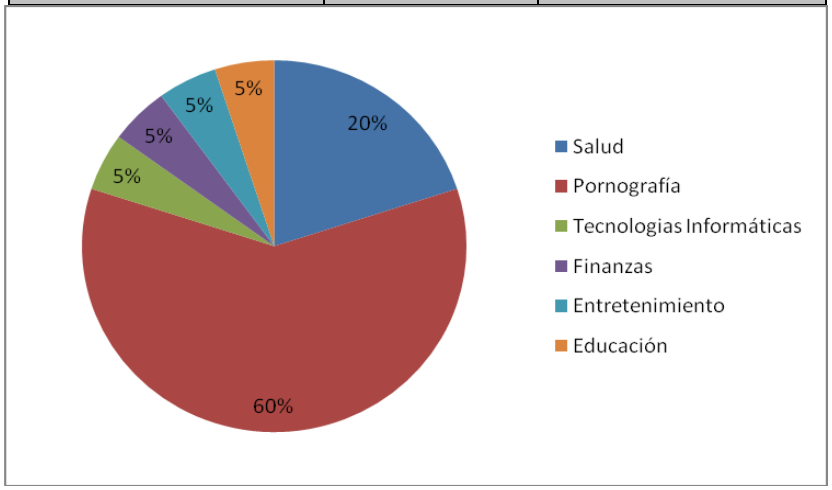


Ilustración 4: Resultado de la encuesta, pregunta # 4

Se puede observar que la mayor parte de encuestados les molesta que llegue a su correo electrónico spam con pornografía, entretenimiento, etc.

5. ¿Conoce usted alguna herramienta para combatir el Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	7	35 %
NO	13	65 %
TOTAL	**20**	**100 %**

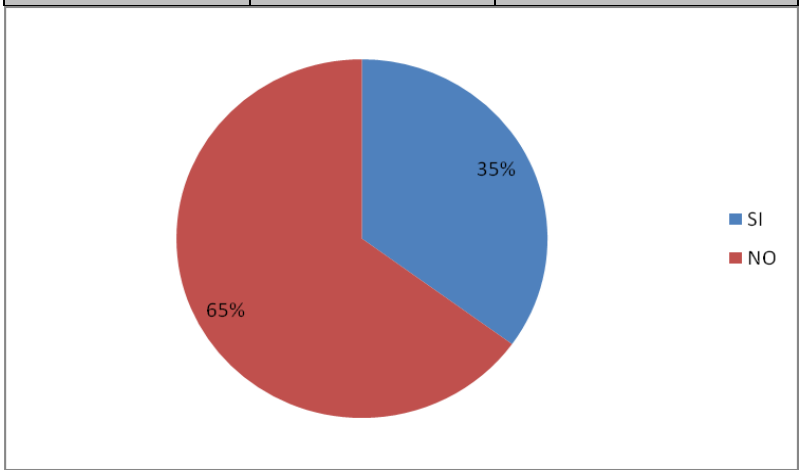


Ilustración 5: Resultado de la encuesta, pregunta # 5

El 65% de los encuestados no tienen conocimiento de alguna herramienta que les ayude a combatir este tipo de correos.

6. **¿Sabe usted como obtiene el spammer (spammeador) su dirección de correo?**

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	4	20%
NO	16	80 %
TOTAL	**20**	**100 %**

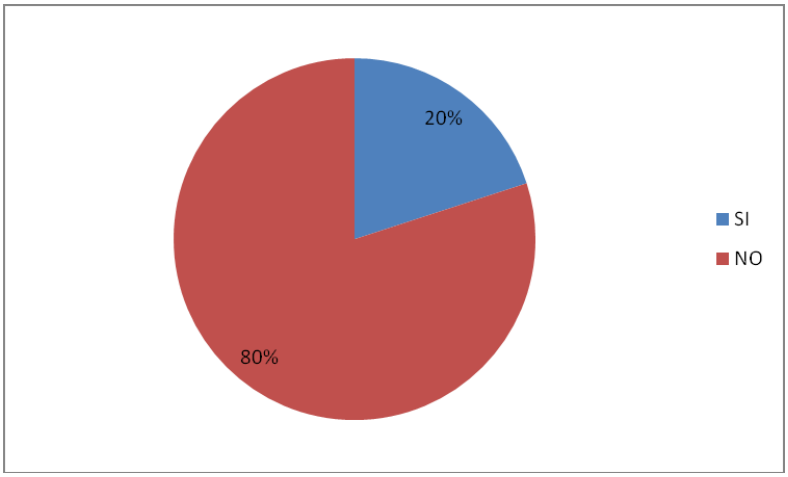


Ilustración 6: Resultado de la encuesta, pregunta # 6

Se puede observar que el 80% de los encuestados no saben como los spammers obtienen sus cuentas de correo y así enviarles spam.

7. ¿Conoce usted las consecuencias de recibir Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	6	30%
NO	14	70 %
TOTAL	**20**	**100 %**

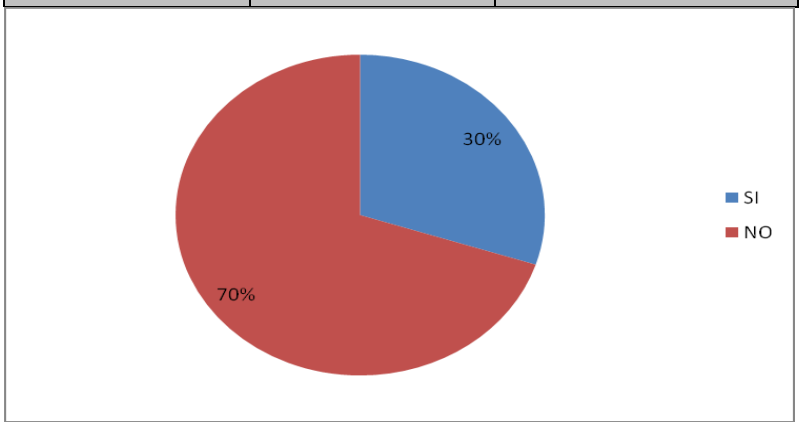


Ilustración 7: Resultado de la encuesta, pregunta # 7

El 70% de los encuestados no conocen de los consecuencias que trae el recibir spam y el daño que pueden causar.

8. ¿Sabe usted como protegerse para no ser víctima del Spam?

	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA
SI	7	35%
NO	13	65 %
TOTAL	**20**	**100 %**

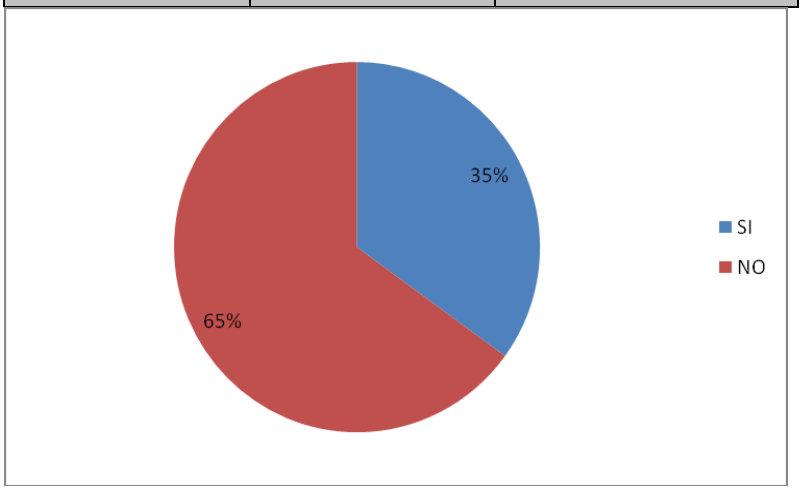


Ilustración 8: Resultado de la encuesta, pregunta # 8

El 65% de las personas encuestadas no conocen como proteger sus cuentas de correo electrónico y no ser víctima de estos mensajes.

CAPITULO IV

TÉCNICAS DE ENVIO Y ATAQUES DE SPAM

INTRODUCCIÓN

Los spammers usan programas y tecnologías especiales para generar y transmitir los millones de mensajes de spam que son enviados cada día. Esto requiere significantes inversiones de tiempo y dinero.

A continuacion se describe las técnicas que utilizan para el enviar y atacar.

4.1 TÉCNICAS DE ENVIO DE SPAM

El envío de Spam se hace a través de los siguientes pasos:

- Recolección y verificación de direcciones de correos electrónicos.
- Creación de plataformas de envío masivo.
- Generación de código para el envío masivo.
- Realizar textos para campañas específicas.
- Enviar el correo no deseado.

4.1.1 RECOLECCIÓN Y VERIFICACIÓN DE DIRECCIONES DE CORREOS ELECTRÓNICOS.

En este paso se recolecta la mayor cantidad de direcciones de correos además información personal de los propietarios de dichos correos y se almacena esta información en la Base de Datos. Los métodos de recolección son las siguientes:

- Adivinar direcciones de correos electrónicos. Se crean direcciones de correos con combinaciones de palabras y números aleatoriamente. Por ejemplo: pablo1@hotmail.com, pedro3@yahoo.com, juan32@usm.cl, etc.

- Escaneo de recursos públicos. Se busca en sitios Web, Foros, Cuartos de Chat, Base de Datos, busca de combinaciones de palabras. Por ejemplo: palabra1@palabra2.palabra3, donde palabra3 es un dominio .com o .info.

- Robo de Base de Datos a los sitios Web, proveedores de Internet, etc.

- Robo de datos personales de usuarios mediante Troyanos. Este método es muy efectivo ya que permite la personalización de los mensajes y la expansión exponencial de la cantidad de direcciones almacenadas.

Luego de haber recopilado las direcciones se deben verificar, para esto se envían correos a las direcciones de la lista y se analiza en el Log del Servidor de Correos las direcciones activas e inactivas y se actualiza la lista de direcciones. Luego de verificar las direcciones activas, se comprueba si los destinatarios abren los correos. Formas de realizar esto son las siguientes:

- Se envían correos con Links a páginas Web especialmente diseñadas con el objetivo de indicar al Spammer si la página ha sido accesada o no. Por ejemplo, el link hacia la página es una parte del e-mail que tiene relación con darse de baja en la suscripción de alguna propaganda, siendo en realidad un link que avisa al Spammer que el correo ha sido leído.

- Un método ya casi ya no se utiliza es la descarga automática de una imagen al abrir un correo electrónico, al descargar la imagen el Spammer detecta que el correo ha sido leído. Las aplicaciones actuales no permiten descargar imágenes automáticamente lo que deja cada vez más obsoleta esta técnica.

4.1.2 CREACIÓN DE PLATAFORMAS DE ENVÍO MASIVO.

En la actualidad, los spammers usan uno de los tres métodos de envíos masivos:

1. Envíos directos desde servidores de correo arrendados. Arrendar servidores es problemático, porque las organizaciones antispam monitorean los envíos masivos y son rápidos para añadir estos servidores a las listas negras. La mayoría de los

proveedores de Internet y programas antispam usan listas negras para identificar el spam: esto significa que una vez que se añade un servidor a la lista negra, ya no puede ser usado por los spammers.

2. Usando retransmisión abierta y proxis abiertos, es decir, servidores que ha sido insuficientemente configurados y por lo tanto están accesibles a cualquiera. Usar la retransmisión abierta y los servidores proxy también requiere tiempo y dinero. Los primeros spammers tenían que crear y mantener robots que buscaran servidores vulnerables en Internet. Luego esos servidores tenían que ser penetrados. No obstante, con mucha frecuencia, después de unos pocos envíos masivos, esos servidores también son detectados e incluidos en las listas negras.
3. Redes bot, redes de equipos zombi infectados por programas maliciosos, por lo general un troyano, que permite a los spammers usar los equipos infectados como plataformas para envíos masivos sin el conocimiento o consentimiento de su propietario.

Como resultado, hoy la mayoría de los spammer prefiere crear o comprar redes zombi. Los autores profesionales de virus usan una variedad de métodos para crear y mantener estas redes:

1. Explotar las vulnerabilidades en los navegadores de Internet, sobre todo de Internet Explorer. Hay cierto número de vulnerabilidades en los navegadores que hacen posible penetrar a un ordenador desde un sitio que el usuario está visitando. Los autores de virus explotan esas brechas y escriben troyanos y otros programas maliciosos para penetrar en los equipos víctimas, otorgando completo acceso y control a los equipos infectados. Por ejemplo, los sitios pornográficos y otros sitios semilegales populares están con frecuencia infectados por programas maliciosos. En 2004 una gran cantidad de sitios fueron penetrados e infectados por troyanos. Después, esos troyanos atacaban los equipos de los usuarios que creían que esos sitios eran seguros.

2. Usar gusanos de correo electrónico y explotar las vulnerabilidades de los servicios de Windows para distribuir e instalar troyanos.
    a. Los brotes virales más recientes han sido causados por amenazas combinadas, que incluían la instalación de una puerta trasera (backdoor) en los equipos infectados. Es más, casi todos los gusanos de correo electrónico tienen un troyano en calidad de "carga útil".
    b. Los sistemas Windows son intrínsecamente vulnerables. Los hackers y los creadores de virus están siempre listos a explotarlos. Las pruebas independientes han demostrado que un sistema con Windows XP sin cortafuegos y antivirus es atacado en los primeros 20 minutos de conectarse a Internet.
3. El software pirata también es uno de los vehículos favoritos para la propagación de código malicioso. Como esos programas son con frecuencia propagados por redes de intercambio de archivos como eDonkey, Kazaa y otros, las redes en sí son penetradas e incluso los usuarios que no usan software pirata son sometidos a riesgo.

4.1.3 GENERACIÓN DE CÓDIGOS PARA EL ENVÍO MASIVO.

Los Spammers deben crear programas capaces de enviar muchos correos en poco tiempo, verificar la validez de una Base de Datos de direcciones, falsificar encabezados de mensajes para hacerlos parecer legítimos, detectar si los mensajes fueron recibidos o no para proceder al reenvío.

4.1.4 REALIZACIÓN TEXTOS PARA CAMPAÑAS ESPECÍFICAS.

Debido a que a la actualidad existen diversas maneras de filtrar correos que contengan gran número de correos con el mismo tipo de mensaje, los spammers deben asegurar de que cada mensaje enviado sea único. Para esto se utilizan las siguientes técnicas:

- Se incluyen reglones de textos invisibles o palabras al azar en los mensajes. El texto invisible se puede hacer fácilmente ya que un mensaje HTML puede contener letras pequeñísimas o textos de color de fondo. Sin embargo, los fabricantes de Anti-Spam han desarrollado técnicas que combaten este tipo de prácticas.

- Se envían Spams gráficos. Este tipo de Spam es más difícil de detectar por los filtros, aun más si son gráficos dinámicos que contienen información destinada a evadir los filtros.

- Se envían Textos Dinámicos. Son utilizados para confundir a los filtros el tiempo necesario para cumplir el objetivo necesario del Spam.

4.1.5 ENVÍO DE LOS MENSAJES

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a Internet, por consumirse gran parte del ancho de banda en mensajes basura.

Una de las formas más comunes para enviar spam es a través de las PCs tomadas para este propósito. La razón, es porque hoy las PCs (generalmente domésticas) cuentan con un gran ancho de banda a Internet y gran capacidad de procesamiento. Además, se tiene la peculiaridad de que las direcciones IP suelen variar por ser dinámicas, esto hace que el equipo no sufra inconvenientes provocados por los filtros de correo pero se utilizan listas negras (donde se marcan las direcciones IP que generan spam). No sólo atacan PCs, también hacen lo mismo con servidores con sistemas operativos como Windows, Linux, y quizás algún otro tipo.[7]

[7] http://www.rediris.es/mail/abuso/doc/spam.pdf

4.2 ATAQUE DE SPAMMERS

4.2.1 COMPONENTES DE UN ATAQUE

Los componentes que intervienen en este tipo de incidentes son:

- **Emisor del ataque** (spammer). Envía un mismo mensaje hacía un gran número de direcciones destino (masa de direcciones). Utilizará cualquier correo de internet desprotegida y mal gestionada.

- **Máquina atacada**. Máquina desprotegida, sin medidas anti-relay y encargada forzosamente a procesar la entrega del correo y de emitir informes de error. Pueden ser varias las máquinas atacadas de forma simultánea.

- **Emisores de fallos de error**. Son las máquinas que emiten el informe de error.
  Son: la propia máquina atacada y cualquier otro servidor de correo que esté recibiendo correo del ataque.

- **Máquina inocente atacada**. Es la receptora de los informes de error producidos en el ataque y de las denuncias. Es la verdadera víctima de este ataque ya que puede ser una máquina correctamente protegida contra el spam.

4.2.2 PROCEDIMIENTO DEL ATAQUE

1. **Elaboración del mensaje**. El Emisor del ataque prepara un mensaje con un campo From (Remitente)[8], quizás pueda añadir tambien un campo Reply-to (Contestar a)[9], ambos generalmente idénticos. Estas direciones suelen ser falsas (podrán ser direcciones correctas e inundar el buzón del inocente propietario de la misma)

[8] En este campo se indica la dirección de mail del remitente

[9] Este campo se utiliza para colocar una dirección alternativa a donde se desea que se envíe la respuesta al mensaje. Este campo es opcional y en caso de no existir se utiliza la dirección del FROM:.

escogidas al azar del estilo fd34rf@dpto.usal.es o incluso el mismo ataque utiliza unas direcciones similares en las que sólo cambian algunas letras.

2. **Ataque a una máquina mal gestionada**. Mediante un procedimiento automático inyectan el mensaje en un servidor desprotegido de Internet (Máquina atacada) con destino a un número elevado de direcciones de correo-e (masa de direcciones). Es fácil que muchas de estas direcciones sean incorrectas.

3. **Procesamiento de errores**. La máquina atacada además de gestionar la entrega de correo a direcciones correctas deberá procesar los errores producidos de las que son incorrectas.

   Algunas de las direcciones a las que se envía el spam serán aceptadas por sus servidores de correo que las encaminarán hasta el servidor final el cual podrá rechazarlo por múltiples motivos y enviará un informe a la máquina responsable de la dirección del campo From.

4. **Informes de error**. Estos informes irán encaminados a la dirección del campo From y la máquina responsable de la misma será la verdadera víctima de este tipo de ataques. Pero dado que la dirección del campo From: es incorrecta ésta máquina inocente generará el clásico informe de error: <<< 550 <j9fyx7429@gugu.usal.es>... User unknown

4.2.3 TIPOS DE ATAQUES

4.2.3.1 ATAQUES DE DIRECTORIO DHA

Los ataques de recolección del directorio ocurren cuando un spammer utiliza direcciones de correo conocidas para generar otras direcciones de correo válidas de servidores de correo empresariales o de ISPs[10]. Esta técnica permite al spammer enviar

[10] Proveedor de Servicios de Internet, es una empresa que brinda conexión a Internet a sus clientes.

correo a direccíones generadas aleatoriamente. Algunas de estas direcciones de correo son usuarios reales de la organización, sin embargo muchas de ellas son direcciones falsas que inundan el servidor de correo de la víctima.

Los "spammers" usan los ataques de directorio para intentar localizar direcciones válidas de correo electrónico mediante adivinaciones en varias permutaciones de nombres de usuario comunes y adjuntando el nombre de dominio.

4.2.3.2 ATAQUES EN REDES SOCIALES

En este mundo de los negocios por internet, el uso de las herramientas tales como Skype, Messenger, Facebook , Twitter y Youtube son casi imprescindibles en los negocios , sin embargo últimamente he visto el mal uso que muchas personas sin conocimiento de marketing ocupan estas herramientas con la sencilla razón de hacer SPAM.

En las, tan de moda, redes sociales como Facebook, MySpace y Twitter muchos de los perfiles son falsos. Casi siempre se utilizan para enviar e-mails con contenido spam o phishing a falsos amigos. La mayoría incluyen enlaces a lugares infectados con malware, virus u otras formas de código sospechoso. Se calcula que hasta un 40% de los nuevos perfiles en Facebook son falsos.

Los spammer han encontrado que las tradicionales formas para enviar spam ya no son tan efectivas en la actualidad, es por ello que están aprovechando las redes sociales. Dichas redes sociales están esforzándose en detectar todos esos perfiles falsos, pero los spamers utilizan robots para rellenar de forma automática es por ello que son tan difíciles de evitar.

Facebook presentó una demanda, el pasado noviembre de 2008, contra un spammer por 1 billón de US$ y ganó. Otras como MySpace también tomaron medidas similares durante el pasado año.[11]

[11] http://www.noticias.com/tecnonews-spamfighter-tuenti-aduena-perfiles-phishing-amigos.2626

Son muchas las veces que los spammer mediante el envío de spam, a través de las redes sociales, infectan ordenadores que ya tienen perfiles creados. A partir de ahí empiezan a enviar mensajes a sus amigos, y éstos los aceptan ya que como llegan de un "amigo", aparentemente son menos sospechosos. Es por ello que probablemente los spammer tendrán más éxito con esta nueva forma de spam a través de las redes sociales durante el 2011 y en los sucesivos años.

CAPÍTULO V

MÉTODOS PARA DETECTAR Y ELIMINAR SPAM

INTRODUCCIÓN

En los últimos años, debido a la proliferación de gran cantidad de mensajes spam en Internet, la utilidad de los sistemas de correo electrónico se ha visto gravemente afectada. Durante estos años, se han logrado grandes avances en la investigación para la creación de filtros antispam. A continuación se revisan los modelos basados en contenido, que aplican distintas métodos para la detección de correo no legítimo.

5. MÉTODOS PARA DETECTAR Y ELIMINAR SPAM

Se han desarrollado varios métodos para filtrar el correo no deseado. Algunas se centran en las cabeceras del mensaje, otras en el cuerpo y otras en el mensaje completo. Los filtros más efectivos suelen utilizar varias técnicas.

5.1 FILTRADO POR CAMPOS DEL MENSAJE DE CORREO ELECTRÓNICO.

Prácticamente todos los clientes de correo electrónico permiten clasificar el correo según la dirección o el dominio del remitente, o por la aparición de ciertas palabras en el asunto o en el cuerpo del mensaje. Estos filtros pueden eliminar un pequeño porcentaje de spam, pero los spammers los derrotan con facilidad falsificando las cabeceras del mensaje y modificando las palabras más relevantes. Además, exigen una configuración totalmente manual. Su mayor utilidad es la creación de listas blancas de remitentes conocidos, cuyos mensajes podrían ser considerados spam por otros métodos.

5.2 ANÁLISIS DE CABECERAS.

Búsqueda de datos falsos en las cabeceras, incluyendo comprobación de que existe la dirección del remitente, de si las estafetas por las que supuestamente ha pasado el correo existen, o si están abiertas, o si hay campos malformados.

5.3 LISTAS NEGRAS Y BLANCAS

Las listas negras y reglas sobre dominios, redes y hosts fue uno de los primeros métodos utilizados para detectar correo spam. Se basan en el uso de reglas simples de exclusión de

mensajes que han sido manipulados o provienen de ciertos dominios, redes o servidores de Internet. Con estas reglas se pueden identificar y clasificar grandes cantidades de correo no deseado, sin embargo, no resulta complicado falsificar y manipular este tipo de información.

Las listas negras de direcciones de spammers son accesibles mediante servicios web o ficheros compartidos a través de los cuales, y de forma remota, se puede consultar si una determinada dirección de correo es remitente de mensajes spam. Algunas de estas listas se encuentran compartidas en forma de ficheros de texto, que contienen remitentes o expresiones regulares acerca de direcciones de correo electrónico.

Como contrapartida, una lista blanca contiene una enumeración de equipos de los que nunca se debe desconfiar, y que mantienen una relación de confianza garantizada a partir de una comunicación anterior. Cada vez que el servidor de correo electrónico recibe un mensaje de un usuario en el que no confía, le envía al remitente un correo en el que le indica que para verificar su identidad, debe seguir un enlace web. Cuando el remitente accede al enlace, el correo electrónico enviado se entrega al destinatario y se establece la relación de confianza. Una vez establecida dicha relación, no se volverá a realizar la verificación de ningún mensaje posterior. Pese a su simplicidad, este tipo de mecanismos son muy difíciles de burlar, aunque se puede perder cierta cantidad de mensajes debido a personas que no desean ser verificadas. En este sentido, un inconveniente a mayores es que los mensajes generados de forma automática, como los boletines de suscripción o los procesos de confirmación de suscripción a listas o servicios electrónicos nunca serán verificados.

5.4 FILTROS BASADOS EN EL CONTENIDO.

Se basan en el estudio del mensaje en sí y suelen ser los más efectivos. La idea básica es que la mayoría del spam intenta transmitir unos mensajes muy concretos y con un tono muy peculiar, así que debe de ser posible distinguirlos de los mensajes deseados que intercambia un usuario con otros.

Los modelos basados en contenido tratan de determinar los atributos comunes a los mensajes spam y legítimos, a partir de una representación en forma de vector de las características de cada correo. Para extraer esta información de un texto, se selecciona una lista de palabras representativas de la legitimidad de los mensajes. Cada mensaje se representa con un vector de números reales o de valores lógicos que contiene, en cada posición, la frecuencia o presencia de los términos seleccionados.

5.5 FILTRADO BAYESIANO

El filtrado bayesiano se basa en el principio de que la mayoría de los sucesos están condicionados y en que la probabilidad de que ocurra un suceso en el futuro puede ser deducido de las apariciones previas de ese suceso. Este mismo método se puede utilizar para clasificar el correo basura. Si algún patrón de texto se encuentra a menudo en el correo spam pero no en el correo legítimo, sería razonable asumir que este correo es probablemente spam. Antes de que el correo electrónico pueda ser filtrado, utilizando este método, el usuario necesita generar una base de datos con palabras y testigos (como el signo $, direcciones IP y dominios, etc.), recogidos de un ejemplo de correo spam y de correo válido (referido como ham). Se asigna entonces un valor de probabilidad para cada palabra o muestra; la probabilidad se basa en cálculos que tienen en cuenta que tan a menudo aparece la palabra en el spam frente al correo legítimo (ham). Esto se hace mediante el análisis del correo saliente de los usuarios y del correo spam conocido. Todas las palabras y muestras de ambos grupos son analizadas para generar la probabilidad de que una palabra concreta apunte que el correo sea no deseado.

El filtrado bayesiano ofrece, por lo tanto, múltiples ventajas que le hacen mejor que otros métodos de detección. En primer lugar, el método bayesiano tiene en cuenta la totalidad del mensaje -reconoce palabras clave que identifican el spam, pero también reconoce palabras que denotan correo válido-. Por ejemplo: no todo el correo que contiene la palabra "gratis" o "dinero en efectivo" es spam. La ventaja del método bayesiano es que considera la mayoría de palabras interesantes (definidas por su desviación de la media) y da como resultado una probabilidad de que un mensaje sea spam. El método bayesiano también reconocería el nombre del contacto de negocio que envió el mensaje, para clasificar, de ese

modo, el mensaje como legítimo. Esto convierte al filtrado bayesiano en una estrategia mucho más inteligente, ya que examina todos los aspectos de un mensaje. Como segunda ventaja importante, un filtro bayesiano está constantemente 'autoadaptándose'. Mediante el aprendizaje del nuevo spam y la salida de nuevo correo válido, el filtro bayesiano evoluciona y se adapta a las nuevas técnicas spam. Por ejemplo, cuando los spammers comenzaron a utilizar "g-r-a-t-i-s" en lugar de "gratis", consiguieron eludir los análisis de palabras hasta que "g-r-a-t-i-s" fue incluido en la base de datos de palabras. El filtro bayesiano advierte automáticamente de estas tácticas; de hecho, si se encuentra la palabra "g-r-a-t-i-s", es incluso un mejor indicador de spam.

El método bayesiano es multilingüe e internacional. Un filtro anti-spam bayesiano, al ser adaptable, puede utilizarse con cualquier idioma. La mayoría de las listas de palabras clave sólo están disponibles en inglés y son, por lo tanto, poco eficaces en regiones de habla no inglesa. El filtro bayesiano también tiene en cuenta ciertas desviaciones del lenguaje o los diversos usos de ciertas palabras en áreas diferentes, incluso si se habla el mismo idioma. Esta inteligencia lo habilita como un filtro para atrapar más spam.

CAPITULO VI

DESARROLLO DE HERRAMIENTAS ANTISPAM

INTRODUCCIÓN

Es importante contar con sistemas que permitan identificar y filtrar el SPAM, algunas herramientas que podemos recomendar para su respectivo análisis y consideración. Para la selección de las 3 herramientas (MailWasher, SpamKiller y Spamfighter) a estudiarse, se consideró lo siguiente:

1. Debe ser una herramienta de filtrado de spam independiente, que comprueba todos los correos entrantes en el servidor, detecta y elimina los mensajes de spam.

2. La eliminación de spam sin que lo recibe en la bandeja de entrada. De esta manera no se descargarán todos los kilobytes en la bandeja de entrada y no verá el molesto correo spam.

3. La herramienta debe analizar el mensaje de "fuera" y "dentro": encabezado, cuerpo del mensaje, y la fuente del mensaje, lista blanca flexible y la lista negra fácil de editar y actualizar también son muy útiles ya que ayudan a ahorrar mucho tiempo al filtrar mensajes de correo electrónico. Un buen software anti-spam debe tener también el filtro bayesiano en su arsenal de herramientas de filtrado de spam.

4. El método más sencillo y seguro a los correos electrónicos vista previa marcados como spam. Inherentes a la tecnología anti-spam es el hecho de que no habrá falsos positivos y falsos negativos, es decir, correo electrónico puede ser marcado como spam, aunque en realidad no es spam, y viceversa.

5. Un software de filtrado de correo no deseado debe proporcionar la posibilidad de recuperar un correo electrónico si se caracterizó por accidente como spam y se encuentra en la papelera.En pocas palabras, un programa anti-spam debe ser un independiente, fácil de usar software suministrado con potentes filtros anti-spam puede ser ajustado por cada usuario para sus necesidades personales.

Las 3 herramientas elegidas cumplen con estos requisitos que son indispensables para la detección y eliminación del spam, es por ello que se prefirió estas herramientas para ser estudiadas.

PROGRAMA	MailWasher	Spam Alarm	Spam Bayes	SpamKiller	SpamFighter	SpamBully	Outlook Spam Filter
Proceso de Descarga	sencillo	sencillo	complejo	sencillo	sencillo	complejo	sencillo
Tamaño de la Descarga	3 MB	10MB	10MB	5MB	10MB	8MB	10MB
Dificultad de Instalación	fácil	fácil	media	fácil	fácil	media	media
Espacion en Disco Duro	4MB	10MB	10MB	10MB	10MB	20MB	15MB
Fácil de Configurar	si	si	no	si	si	no	si
Compatible con Windows 7 y Vista	si	no	no	si	si	si	no
Interfaz Amigable	si	si	no	no	si	no	no
Outlook- Outlook Express	si	si	si	si	si	no	si
Compatible con Hotmail, Yahoo, Gmail	si	no	no	si	si	si	no
Protección de múltiples cuentas de	si	no	no	si	si	si	no
Actualización automática gratis	si	no	no	si	no	no	no
Cliente de correo libre de publicidad	si	si	si	si	si	si	si
Filtrado de Mensajes	si	si	si	si	si	si	si
Filtrado basado en contenido	si	si	si	si	si	si	si
Filtrado Bayesiano	si	no	no	no	si	no	no
Filtrado mediante Listas Negras	si	si	no	si	si	no	no
Filtrado mediante Listas Blancas	si	si	no	si	si	no	no
Filtrado de phising	no	no	no	si	si	no	no
Interfaz con múltiples idiomas	no	no	no	no	si	no	no
Versión Gratis	si	si	si	si	si	si	si
Versión en Español	no	no	no	no	si	no	no
Precio	$ 41,99	$75,00	$30	$35,40	$29,00	$40,00	$33,50

El cuadro comparativo nos muestra todas las características que debe tener una buena herramienta que nos ayude a combatir el spam, es por ello que las 3 herramientas que se encuentran marcadas de color celeste son las más eficientes, por lo tanto serán las que se investigarán para conocer su funcionamiento.

6. DESARROLLO DE HERRAMIENTAS ANTISPAM

6.1 MAILWASHER 5.0

Este programa es bastante popular entre los usuarios del correo electrónico; se destaca porque es capaz de importar automáticamente las cuentas de correo (dependiendo del cliente de correo que se use) y de eliminar un mensaje o "rebotarlo" contra su remitente. La ventana principal de la interfaz incluye la información principal de los correos tal como remitente, asunto, fecha de envío y cuenta de correo; además ofrece un dato interesante como es el estado (*Status*), donde informa si es un posible spam, un mail de trabajo, normal, etc.

Mail Washer sirve para conectarse al servidor de correo, antes de hacerlo con el programa habitual, para revisar los mensajes, seleccionar el correo basura y el correo legítimo y borrar todo lo que no queremos. Luego, podemos descargar los mensajes con nuestro programa de correo, como Outlook o Thunderbird, sabiendo que vamos a recibir sólo los mensajes que deseamos.

Es compatible con: Windows 7, Vista, XP, 2000 Su última versión estable fue liberada hace poco, donde mejoran su compatibilidad con algunos clientes de e-mail.

MailWasher es compatible con los siguientes clientes y servicios de correo electrónico:

- Incredimail
- Outlook
- Outlook Express
- Windows Mail

- Windows Live Mail
- Gmail (Google Mail)
- Yahoo! Mail
- Windows Live Mail

6.1.1 VENTAJAS DE MAIL WASHER

- Sus bajos requisitos para funcionar, apenas 4 MB de memoria RAM e igual cantidad de espacio en disco duro bastan para tener una instalación exitosa, así también una conexión a internet activa es necesaria para el correcto funcionamiento de la aplicación.

- Marcado y separación del correo normal del basura en base a listas de correos y dominios amigos, listas negras, filtros personalizables enfocados al reconocimiento de frases y remitentes, filtro Bayesiano.

- Papelera de reciclaje integrada, por si se borra algún mensaje erroneamente y se desea recuperarlo.

- Simplicidad en el uso, gracias a su interfaz amigable y bien organizada.

- Resaltado de los mails por colores para mayor reconocimiento, rojo para el spam, verder para el legítimo.

6.1.2 DESVENTAJAS DE MAIL WASHER

- No es un software gratuito, aunque existe una versión libre que cuenta con todas sus funciones.

6.1.3 INSTALACIÓN Y FUNCIONAMIENTO

El Mail Washer se puede descargar en la propia página de los creadores, se puede realizar una descarga gratis y probar el producto sin límite de funcionalidades. No obstante, el precio es bastante razonable, en relación al trabajo que puede ahorrarnos.

6.1.3.2 FUNCIONAMIENTO

En la primera ejecución del programa pide que configuremos las cuentas de correo electrónico que queremos revisar. Esa configuración inicial puede realizarla automáticamente obteniendo los datos de las cuentas de correo electrónico que tenemos configuradas en nuestro ordenador. Por lo que se hace muy sencillo empezar a trabajar. Lo único que pedirá son las claves de las cuentas de correo ha configurado.

El resultado sale muy rápido. Las líneas en verde, en principio, son correos de amigos o de confianza. En la columna status aparece 'Friend', porque anteriormente ya lo hemos marcado así. Si el programa no sabe cómo actuar con un correo, la línea Status aparece en blanco, con el botón derecho del ratón sobre esa línea, nos sale un menú contextual, donde elegimos 'Add to friends list' o pulsamos + para agregar el remitente a la lista de amigos, o elegimos 'Add to blacklist' o pulsamos - para añadir el remitente a la lista de spam o enemigos. En dicha columna aparecerá 'Blacklist', si previamente hemos indicado que es spam, o simplemente, no nos agrada esa persona, o también, porque el remitente está incluído en las bases de datos de spammers que ya lleva incorporadas este programa. Podemos dejarlo así o cambiarlo.

Lógicamente, al principio de usar este programa, nos llevará un poco de tiempo ir añadiendo amigos o enemigos a nuestra lista, pero afortunada o desafortunadamente, no son tantos, y hay que ir haciéndolo por cada remitente, no por cada correo. También podemos añadir a la lista de amigos o enemigos un dominio entero, si es nuestro gusto.

Bien, después de repasado el correo, en la columna 'Delete', nos quedarán marcados o tildados para borrar los correos de quien esté en 'Blacklist', pero además, podemos marcar para borrar todos los que queramos, aunque sean amigos. Del mismo modo, podemos desmarcar un correo spam, si se nos antoja recibirlo.

6.2 SPAMKILLER 2.87

SpamKiller es una de las mejores utilidades antispam que existen. Antes de dejar pasar un correo comprueba que el mensaje o el remitente no esté clasificado como “no deseado” en

su base de datos, formada por una gran cantidad de filtros constantemente actualizados, lo que hace que sea mucho mas eficaz. Éste programa filtra los mensajes electrónicos que llegan de acuerdo a una extensa lista de tipos de mensajes de correo basura que puede ser modificada por el usuario, el cual puede definir además sus propias reglas de filtro de acuerdo a los criterios que él mismo considere relevantes. Una vez marcado algún mensaje como spam, éste se puede borrar o dejar marcado como spam dejándolo en la bandeja de entrada para una posible revisión posterior.

6.2.1 VENTAJAS

- Filtrando – las opciones de filtración avanzadas proporcionan nuevas técnicas de filtración, incluyendo la ayuda para la filtración del meta-character y la identificación del texto de los desperdicios.

- Enchufe del hojeador de Phishing – de AntiPhishing vía una barra de herramientas de Internet Explorer identifica y bloquea fácilmente Web site phishing del potencial.

- Integración de Microsoft Outlook y de Outlook Express – la barra de herramientas proporciona una carpeta dentro de su cliente del correo al Spam del bloque directo.

- Instalación – disposición y configuración aerodinámicas. La detección automática de la cuenta asegura la disposición, la configuración, y la integración lisas con cuentas de correo electrónico existentes.

- Actualizaciones – las auto-actualizaciones funcionan silenciosamente en el fondo, siempre vigilante para reducir al mínimo su exposición a las amenazas emergentes del Spam.

- Interfaz – interfaz utilizador intuitivo para mantener su computadora libre de Spam.

- Ayuda – liberar el soporte técnico inmediato vivo de la mensajería y del email para fácil, pronto, y vivir servicio de atención al cliente.

- Spam el proceso de mensaje – por abandono, se marcan con etiqueta como [Spam] y se ponen los mensajes del Spam en la carpeta de SpamKiller en perspectiva y Outlook Express, o su Inbox. Los mensajes marcados con etiqueta también aparecen en la página aceptada del email.

6.2.2. DESVENTAJAS

- Software disponible solo en inglés.

6.2.3 FUNCIONAMIENTO

SpamKiller garantiza un 99 % de efectividad en la detección de SPAM utilizando 3 módulos que combinan las soluciones más efectivas contra la publicidad masiva:

- Módulo Razor y DCC, se trata de bases de datos centrales que contienen las marcas o "signatures" de e-mails no deseados enviados con anterioridad a miles de servidores de todo el mundo. Este registro se actualiza automáticamente cada 15 minutos.

- Módulo Black Lists, se trata de listas de mail servers con Redireccionamiento Abierto u "Open Relay" que habitualmente son utilizados para el envío de SPAM, de esta forma se deniega el ingreso de correo proveniente de estos orígenes.

- Módulo SpamAssassin, es el componente principal de filtrado de excelente rendimiento y capacidad de detección. Realiza un análisis del contenido de los correos (la cabecera de los mensajes, el cuerpo de éstos, y la dirección de origen de la conexión SMTP) para distinguir un correo deseado de uno no deseado y de esa forma poder eliminarlo. Para este proceso, además de tomar al módulo Razor y DCC como fuente, utiliza métodos heurísticos que le permiten detectar correo no

deseado aunque su contenido o "signatura" haya sido modificado en parte (técnica habitual del spam para pasar los filtros más comunes). Por otra parte, y con la ayuda del módulo Black Lists, basándose en la cabecera del e-mail detecta de donde proviene y de que servidor ha sido enviado.

6.3 SPAMFIGHTER 4.1.8.4

Anti-Spam para Outlook, Outlook Express, Windows Mail y Mozilla Thunderbird que automática y eficientemente filtra el correo no deseado e intentos de estafa por phishing. Siempre que se reciba nuevo correo, éste será examinado automáticamente por SPAMfighter, y si es spam (correo no deseado), será trasladado a su carpeta de spam.

6.3.1 VENTAJAS

- Rápido, muy fácil de configurar, y aún más fácil de usar.
- Protección de todas las cuentas de correo en el mismo PC.
- Protege contra el "Phishing", robo de identidad y otros tipos de estafas electrónicas.
- Lista Negra de dominios y direcciones.
- Denuncia del abuso de spam con un sólo clic.
- Una herramienta única del Filtrado de Idioma ayudará a detectar los e-mails escritos en un determinado idioma.

- Idiomas disponibles Español**,** Inglés, Alemán, Francés, Italiano, Griego, Chino, Japonés, Holandés, Sueco, Noruego, Finés, Ruso, Búlgaro, Portugués, Checo, Tailandés, Turco, Vietnamita y Danés.

6.3.2 DESVENTAJAS

- No es un software gratuito, aunque existe una versión libre que cuenta con todas sus funciones.

6.3.3 FUNCIONAMIENTO

Su modo de funcionamiento es el siguiente: en cuanto un correo llega y el servidor Exchange lo envía a sus destinatarios, construye una firma única para cada mensaje y lo envía al servidor SPAMfighter para que sea evaluado. Si el servidor SPAMfighter determina que el mensaje es spam, y mueve a su carpeta correspondiente.

SPAMFIGHTER REQUIERE:

Sistema Operativo: Windows 2000, XP, Vista o Windows 7 (32 y 64bit)

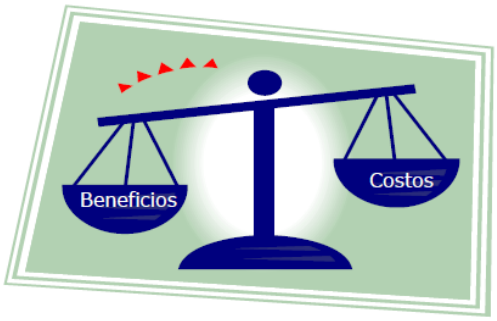
Espacio en Disco: 10MB

Memoria: 128 MB mínimo.

PROGRAMA			
Proceso de Descarga	**Sencillo**	**Sencillo**	**Sencillo**
Espacion en Disco Duro	**4MB**	**10MB**	**10MB**
Fácil de Configurar	✓	✓	✓
Compatible con Windows 7 y Vista	✓	✓	✓
Interfaz Amigable	✓	✓	✓
Outlook- Outlook Express	✓	✓	✓
Protección de múltiples cuentas de correo	✓	✓	✓
Actualización automática gratis	✓	✓	✓
Cliente de correo libre de publicidad	✓	✓	✓
Filtrado de Mensajes	✓	✓	✓
Protege contra el "Phishing", robo de identidad y otros tipos de estafas electrónicas.	✗	✓	✓
Interfaz con múltiples idiomas	✗	✗	✓
Versión Gratis	✓	✓	✓
Precio	**$41.99 USD**	**$35.40 USD**	**$29.00 USD**

6.4 ANALISIS COSTO BENEFICIO

El proceso de generación de un aplicativo de software encierra un conjunto de actividades, una de las primeras para el usuario es el de resolver un dilema nada sencillo, como el de determinar si es conveniente entrar en un proyecto de desarrollo de software o adquirir uno producto terminado.



Descripción del Modelo en el caso de una empresa Mediana.

Con esta introducción de lo que interviene en un Análisis de Costo-Beneficio, se describen a continuación los elementos que deberán contemplarse en la evaluación:

COSTOS:

	MAILWASHER	SPAMKILLER	SPAMFIGHTER
Licencia de Actualización y Mantenimiento por 1 año	**$41,99**	**$ 35,40**	**$29,00**
Instalación y Puesta en Producción	**$50,00**	**$50,00**	**$50,00**
Capacitación	**$50,00**	**$50,00**	**$50,00**
TOTAL	**$141,99**	**$135,40**	**$129,00**

Lista de Beneficios Intangibles

SOLUCIÓN DE SOFTWARE ANTI-SPAM brindará protección contra malware y otras amenazas, a las estaciones de trabajo y servidores; mitigando el riesgo de que se afecte la integridad de la información y el normal desarrollo de las actividades de la empresa.

Mejora de Procesos.- Conducen a reducción de tiempo y recursos

Disponer de Sistemas Antispam.- Mejora el rendimiento de la empresa.

Personal Eficiente.- Personal al funcionar en un entorno de herramientas antispam mejorará su rendimiento y no y desperdiciara su tiempo leyendo y borrando correos que no le interesan.

Protección contra correo no deseado

Protección antivirus

Protección contra el software espía (archivos adjuntos)

Protección contra ataques de negación de servicio

Brindar seguridad a los equipos de cómputo dentro de la institución contra virus y Spam. Contar con un Software que tenga herramientas que ayude a gestionar la seguridad de la información.

Protección efectiva y eficiente durante las 24 horas los 7 días de la semana.

CAPITULO VII

CONSECUENCIAS DEL SPAM

RECOMENDACIONES PARA NO SER VÍCTIMA DE SPAM

INTRODUCCIÓN

Se han identificado algunos efectos negativos y problemas que son generados por el fenómeno del spam, así mismo se da a conocer algunas recomendaciones para evitar ser víctimas de este tipo de correos.

7.1 CONSECUENCIAS DEL SPAM

Se han identificado algunos efectos negativos y problemas que son generados por el fenómeno del spam:

El usuario que lo recibe:

- Pierde tiempo y dinero al descargar mensajes que no solicitó.
- Es molestado permanentemente con publicidad de cosas que no le interesan.
- Puede llegar un momento en que reciba más Spam que mensajes que realmente le interesan.
- Gran parte de los proveedores de Internet limita el tamaño del buzón del usuario en su servidor. Si el número de spams recibidos es muy grande el usuario corre el riesgo de tener su buzón lleno de mensajes no solicitados. Si esto ocurre, el usuario ya no podrá recibir e-mails y, hasta que pueda liberar espacio en su buzón, todos los mensajes recibidos serán devueltos al remitente. El usuario también puede dejar de recibir e-mails en los casos donde estén siendo utilizadas reglas antispam ineficientes, por ejemplo, clasificando cómo spam algunos mensajes legítimos.
- El spam ha sido ampliamente utilizado como vehículo para diseminar por internet esquemas fraudulentos, que intentan inducir el usuario a visitar páginas clonadas de instituciones financieras o a instalar programas maliciosos diseñados para hurtar datos personales y financieros.

A empresas:

- Afecta el tiempo empleado por los usuarios en leer, borrar, denunciar, filtrar etc. y también el tiempo de los responsables de la gestión de los servidores de correo.

- Puede llegar a dañar la infraestructura informática, por un uso inútil de la banda ancha, la denegación de servicio por saturación o la transmisión de virus y gusanos.
- Afecta la productividad empresarial.
- Incremento de la propagación de virus informáticos.

La empresa o persona que lo envía:

- Podrá promocionar su negocio y tal vez vender un poco pero la mayoría de los receptores del Spam sólo tendrán una imagen negativa.
- Su servidor podrá dar de baja su cuenta de correo electrónico para evitar que el Spam afecte su rendimiento y para no figurar en listas negras.

Todos los usuarios de Internet:

- Según una nota publicada en Terra "500 millones de avisos personalizados bombardean cada día las casillas de email de todo el mundo, según un estudio de la Comisión Europea. Esto significa un costo de unos 9,360 millones de dólares al año para los usuarios, en función del tiempo de conexión utilizado". [12]

Esto nos da una idea de cómo esta práctica afecta el rendimiento de toda la red.

7.2 RECOMENDACIONES PARA NO SER VÍCTIMA DE SPAM

Se requiere de múltiples frentes de batalla, definitivamente se trata de un amplio conjunto de factores que intervienen en el fenómeno del spam y por consiguiente no basta con atacar un solo punto, hay que trabajar paralelamente en los puntos que hacen que el spam tome cada vez más fuerza y tratar de debilitarlos en la medida de lo posible. Se estudiaron los puntos más fuertes y sobre ellos se propone focalizar esfuerzos a través de las siguientes recomendaciones, clasificadas de acuerdo a los principales focos o frentes sobre los que se

[12] http://www.riuady.uady.mx/spam/consecuencias.php

puede trabajar, para atacar y tratar de minimizar el impacto que actualmente genera el spam.

Se debe crear conciencia en los usuarios finales del correo, mostrarles las consecuencias y hacer recomendaciones en cuanto al uso y manejo de los mensajes que llegan a su buzón, con el fin de minimizar los riesgos que nos pueden hacer más vulnerables al spam; entre las principales recomendaciones están:

- No publicar la dirección de correo electrónico en páginas Web, o en caso de ser necesario, mostrarla en una imagen.
- Participar en foros que usen moderador y rechazar correos y mensajes de usuarios no suscritos a la lista.
- No reenviar mensajes que hagan parte de una cadena de correo electrónico.
- No hacer envíos en los que sea necesario incluir muchas direcciones de correo y, si es indispensable hacerlo, usar la opción de copia oculta para que no sean visibles las demás direcciones a las personas que seguidamente recibirán ese mensaje.
- Si necesita reenviar un correo que ya contiene alguna dirección en el mensaje, en importante asegurarse de borrarlas antes de enviarlo.
- Al llenar un formulario, abstenerse de dar la dirección de correo. Si es necesario, es recomendable utilizar una redirección temporal, o una cuenta gratuita "extra". Sin embargo, es mejor y mas seguro para evitar ser bombardeado por spam confirmar la seriedad del sitio.
- Leer los correos de remitentes sospechosos como texto, y no como HTML, aunque definitivamente lo mejor es no leerlos o borrarlos inmediatamente para evitar ser víctimas de los diversos ataques a la seguridad informática especialmente spam y virus informáticos.
- No enviar ni responder mensajes al spammer, aunque prometan dejar de enviar spam si se lo hace (esto lo hacen a través de enlaces que normalmente dicen unsubscribe, remove, etc). Al establecer contacto, sólo se está confirmando que la cuenta existe, es auténtica y está activa, como se mencionó anteriormente.
- Tener siempre al día las actualizaciones de seguridad del sistema operativo.

- Instalar software de seguridad tal como cortafuegos (firewall), antivirus, antiSpyware, antiSpam, y mantenerlos siempre activados y actualizados.
- Es conveniente disponer de más de una cuenta de correo. Una para recibir correo serio o aquel que se da a conocer a los conocidos o empresas para que nos envíen correo que resulta "importante". El otro se recomienda utilizar para participar en foros o demás medios. Esta segunda cuenta seguramente será un blanco perfecto para recibir spam.
- Montar filtros o reglas en el correo para no recibir o borrar directamente mensajes procedentes de una dirección concreta. Si se hace esto, se recomienda tener mucho cuidado ya que se puede eliminar correo que puede ser de utilidad.
- No dejar la dirección de correo electrónico en cualquier foro o formulario si no es absolutamente necesario; si requiere hacerlo, se recomienda escribir la palabra "arroba" en lugar del símbolo @, de este modo se evita que sea capturada la dirección por algún programa generador de spam. Hay que recordar que ésta es información que puede ser captada y robada por los programas diseñados por los spammer comúnmente llamados arañas.
- Para evitar contribuir a la difusión de estos correos spam, es importante no creer cualquier mensaje que llegue a la bandeja de entrada por muy emotivo que sea su contenido pues generalmente no se trata de mensajes y casos reales. Lo único que se logra con reenviarlos es facilitar direcciones de correo al spammer.
- Definir y poner en práctica políticas de uso de correo electrónico.
- No realizar ninguna compra desde un correo no solicitado.
- Evitar previsualizar los mensajes, pues muchos spammers usan técnicas publicitarias que pueden monitorizar cuándo se previsualiza un mensaje, independientemente de si lo ha abierto o leído.
- Intentar localizar la casilla destinada en algunos sitios y/o mensajes para aprobar el envío y recibo de más información y asegurarse de que está desactivada.[13]

[13] http://www.zonavirus.com/articulos/consejos-para-evitar-el-spam.asp

CAPÍTULO VIII

CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

Con la realización y culminación de la presente investigación se ha podido ampliar el concepto de Spam y las maneras de cómo llegan estos mensajes a nuestras cuentas de correo electrónico, y como podemos protegernos para no ser víctimas de este fenómeno.

Se ha podido encontrar algunas soluciones para el spam como son las herramientas investigadas las cuales se encargan de analizar cada uno de los emails que llegan al usuario, para identificar si son o no spam. Esos servidores remotos utilizan grandes bases de datos con información (direcciones IP, nombres, textos, etc.) para identificar el correo no deseado.

A pesar de los grandes esfuerzos que hacen las empresas y consumidores, el correo no deseado continúa proliferando porque el aspecto económico de éste sigue siendo muy atractivo. El aspecto económico del correo no deseado sigue siendo difícil de combatir, casi que imposible, puesto que los creadores de spam pueden obtener casi gratis listas de millones de direcciones electrónicas recopiladas. La única barrera para combatir este fenómeno son los filtros contra correo no deseado.

8.2 RECOMENDACIONES

Al culminar esta investigación se ha podido conocer los imnumerables sistema de filtrado anti spam, y las recomendaciones que podemos seguir para no seguir siendo víctimas de estos mensajes.

Es importante y necesario, para pensar en una salida al problema del spam, penalizar a la persona o personas que se dedican a esta tarea, pues es un hecho que el spam es una amenaza a la viabilidad del Internet como un medio efectivo de comunicación, comercio electrónico, y productividad, y mientras no se penalice es difícil pensar en una mejora.

Es absolutamente necesaria la creación de una cultura de uso adecuado de los medios electrónicos, misma que debe ir dirigida tanto a usuarios, como a los proveedores de servicio de internet. Los sistemas contra el spam además de ser un mecanismo de control, deben ser una herramienta para que los ISPs puedan medir la dimensión que el spam representa en su propia red, determinando en consecuencia las medidas a seguir.

GLOSARIO

Firewall: Cortafuegos, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Hackers: es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto.

HTML: lenguaje de marcado de hipertexto, es el lenguaje de marcado predominante para la elaboración de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes.

IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos.

Links: es un navegador web de código abierto en modo texto y gráfico a partir de su versión 2 en modo terminal.

Phishing: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas.

SMTP: Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras.

Spammer: Persona o grupo dedicados a la distribución de correo electrónico no deseado, spam. La actividad suele resultarles sumamente lucrativa, pero está muy mal vista por la mayoría de los usuarios y empresas de internet, de hecho es ilegal en muchos países.

Troyanos: se denomina a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños.

Usenet: es uno de los sistemas más antiguos de comunicaciones entre redes de computadoras, aún en uso. Permite a un usuario intercambiar opiniones y experiencia con otras personas interesadas en el mismo tema específico que él.

BIBLIOGRAFÍA

http://www.espectador.com/spam/servidor.htm

http://pymecrunch.com/spam

http://www.fundeu.es/recomendaciones-S-spam-14.html

http://www.rompecadenas.com.ar/spam.htm

http://www.iec.csic.es/criptonomicon/spam/

http://www.segu-info.com.ar/malware/spam.htm

http://www.masadelante.com/faqs/que-es-spam

http://www.internetglosario.com/560/Spam.html

http://www.datacraft.com.ar/internet-spam.html

http://es.kioskea.net/download/descargar-1301-mailwasher-free

http://tukero.blogspot.com/2010/12/mailwasher-pro-2011-1050.html

http://www.gratisprogramas.org/descargar/mailwasher-pro-6-5-4-portable/

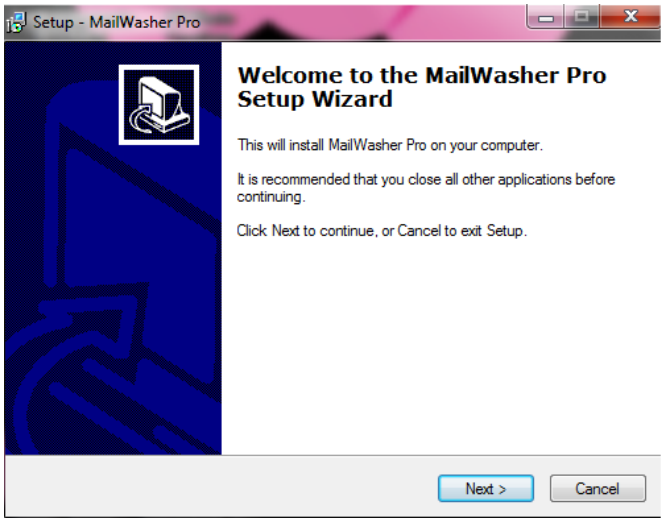
http://www.informatica-hoy.com.ar/spam/Problemas-causados-por-el-SPAM.php

http://www.conectu.com/v4/es_articulos.php?a=113

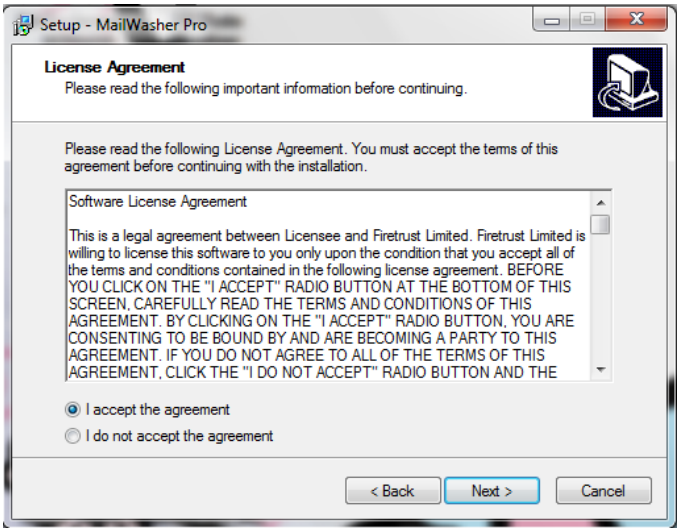
ANEXOS:

ANEXO 1: MANUAL DE INSTALACIÓN Y FUNCIONAMIENTO DE MAILWASHER:

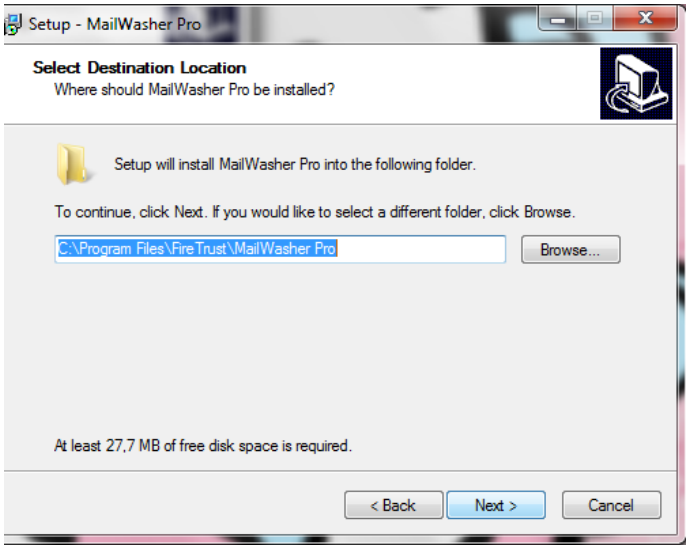
Acontinuación se detalla paso a paso la instalación de Mail Washer:



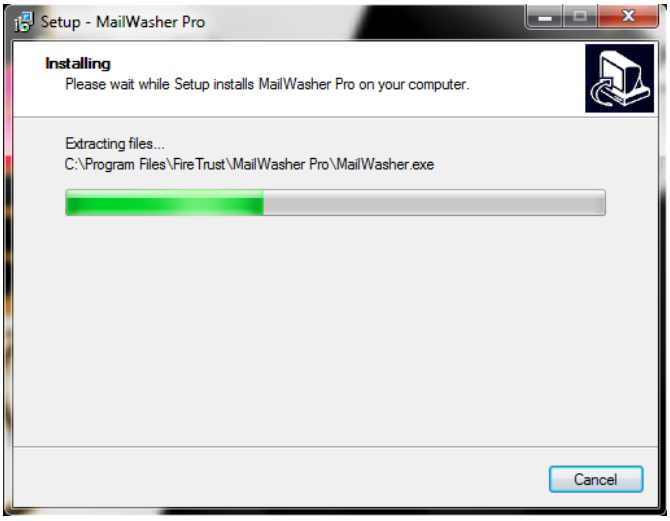
En este paso aceptamos los términos y condiciones del programa:



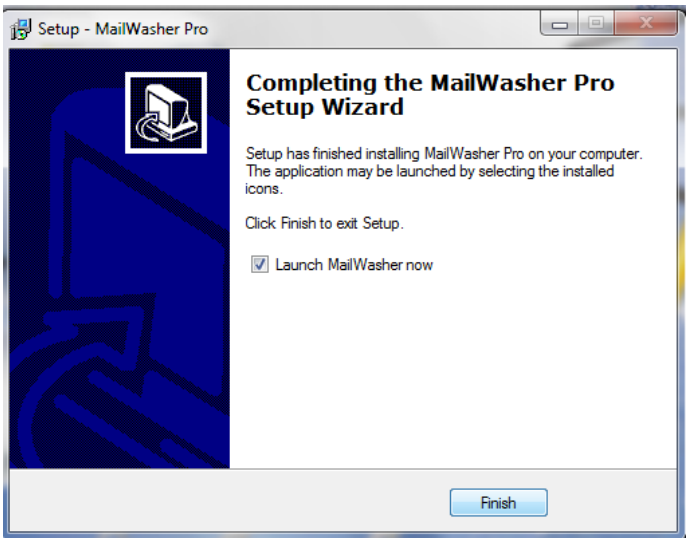
En este paso damos click en el botón siguiente para proceder con la instalación:



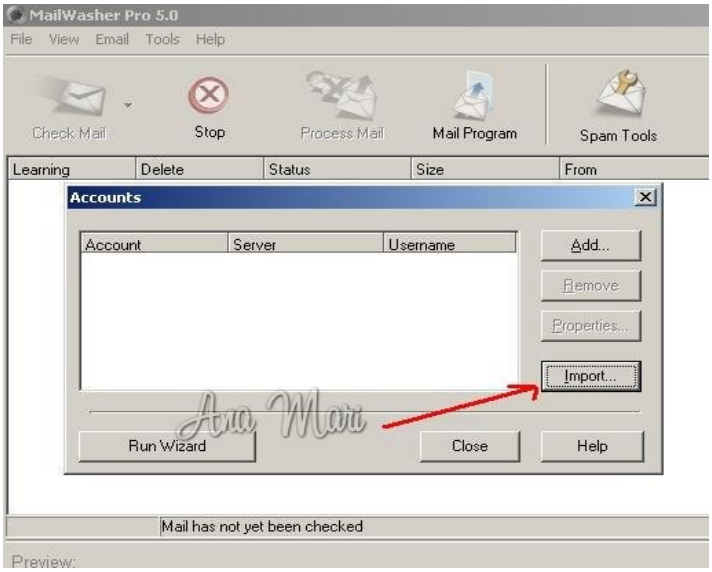
En este paso Mail Washer esta en proceso de instalación:



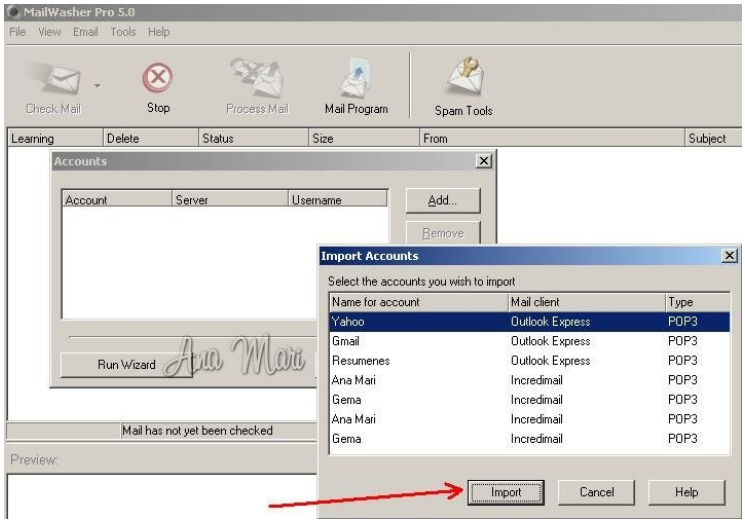
Mail Washer se instaló correctamente:



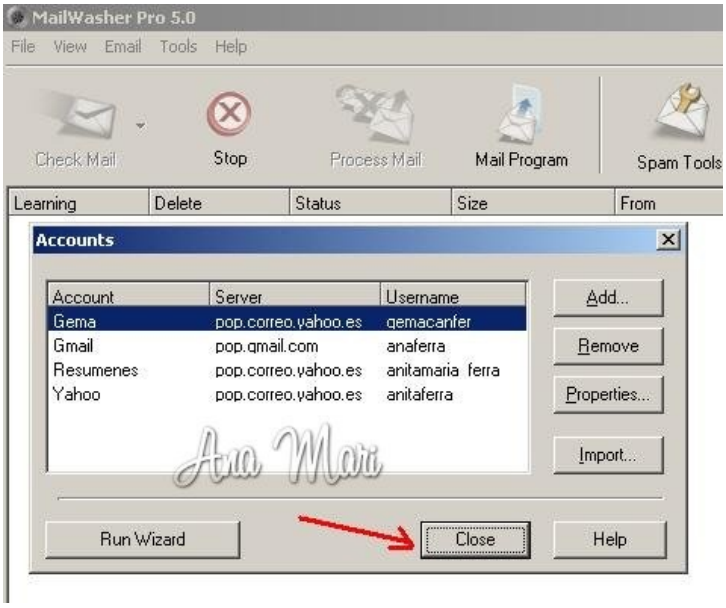
Una vez instalado, en la primera ejecución del programa nos pide que configuremos las cuentas de correo electrónico que queremos revisar. Esa configuración inicial puede realizarla automáticamente obteniendo los datos de las cuentas de correo electrónico que tenemos configuradas en nuestro ordenador. Por lo que se hace muy sencillo empezar a trabajar. Lo único que nos pedirá son las claves de las cuentas de correo ha configurado.



Pulsamos sobre 'Import', y nos aparece lo siguiente:



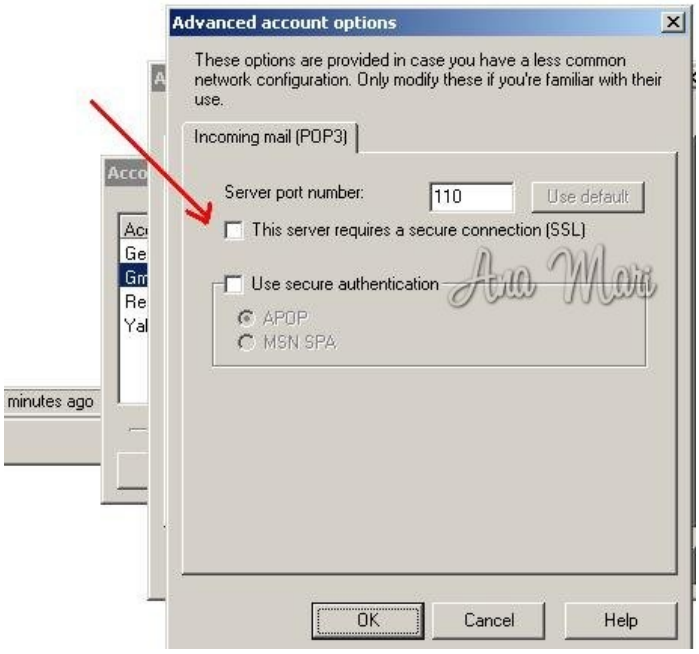
Seleccionamos la cuenta que queramos importar, y le damos de nuevo a 'Import'. La cuenta aparecerá en la ventana anterior.



Le damos a 'Close', y ya están nuestras cuentas configuradas.

A veces, hay que completar algún detallito, por ejemplo, para ultimar una cuenta de gmail, pulsamos F8, seleccionamos la cuenta en cuestión, pulsamos 'Properties' (esto es así cada vez que queramos cambiar algo en alguna de nuestras cuentas), pestaña 'Incoming mail',

Botón 'Advanced account options', y nos sale esto:

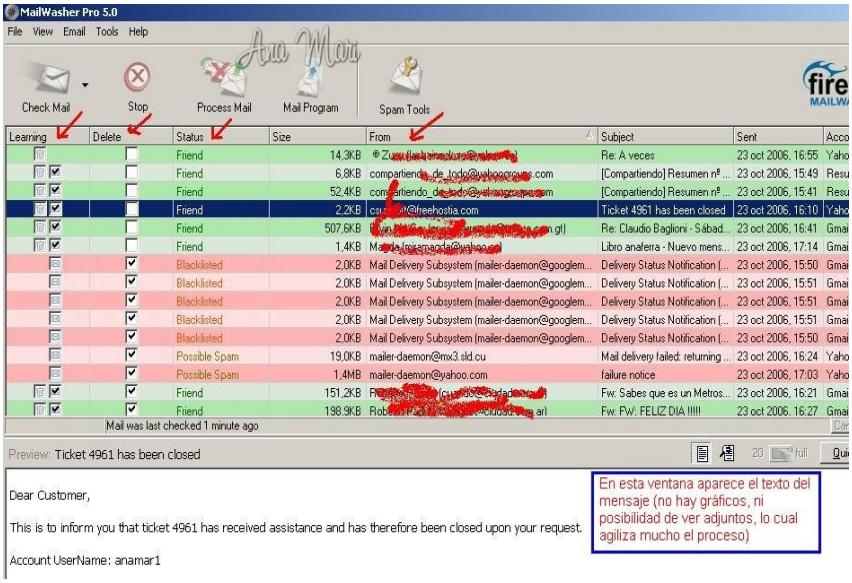


Marcamos o tildamos la casilla señalada, y guardamos pulsando en 'OK', de nuevo 'OK', y 'Close'.

Con alguna otra cuenta, si no funciona, ir probando tildando y destildando cualquiera de estas dos casillas, hasta que consigamos ver los correos, de la siguiente manera:

Pulsando el icono 'Check mail', nos mirará todas nuestras cuentas, pero si le damos a la flechita negra que hay justo a la derecha del icono, podremos seleccionar las cuentas una por una.

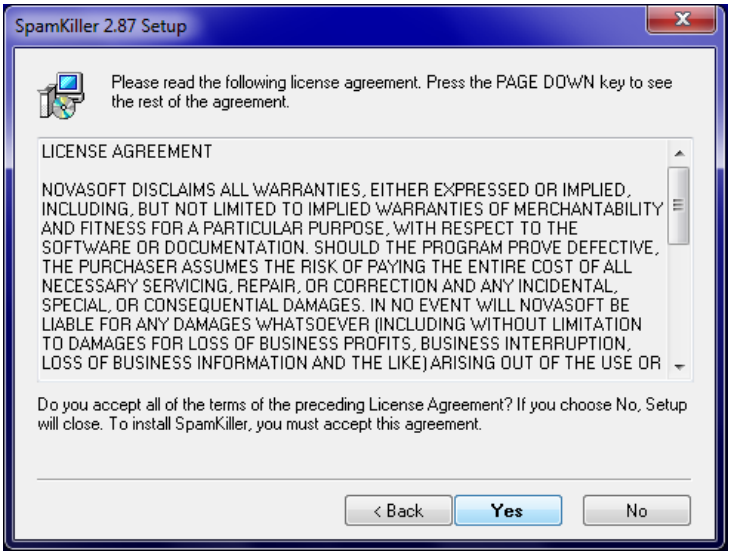
El resultado será algo así:



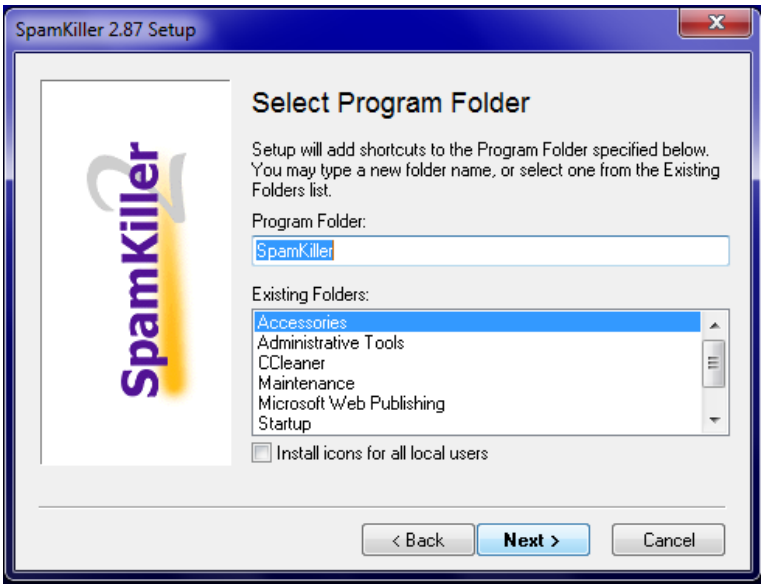
ANEXO 2: MANUAL DE INSTALACIÓN Y FUNCIONAMIENTO DE SPAMKILLER:

En esta primera pantalla solo tenemos que dar click sobre **Next**

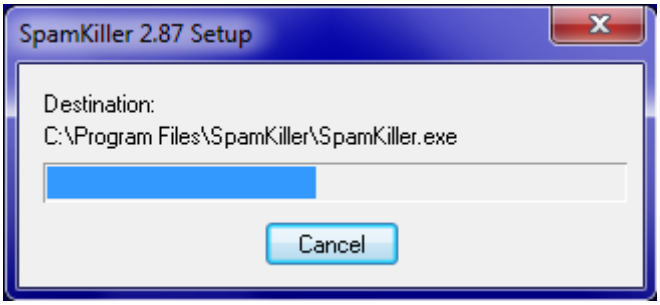
En este paso aceptamos los términos y condiciones del programa:



En este paso damos click en el botón siguiente para proceder con la instalación:



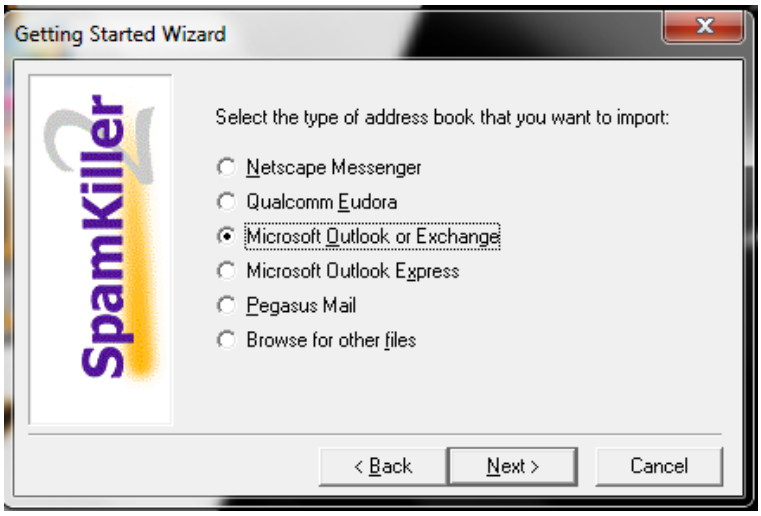
El programa se esta instalando:



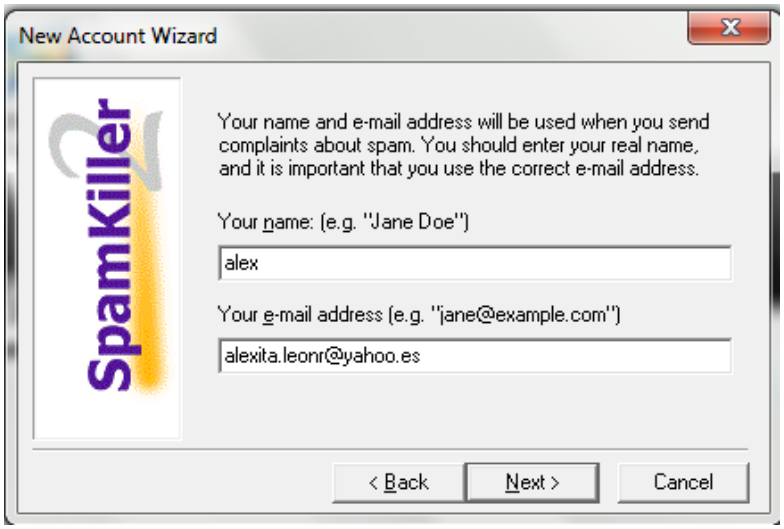
FUNCIONAMIENTO:

La primera pantalla de bienvenida del programa, damos click en Next para continuar con la configuración:

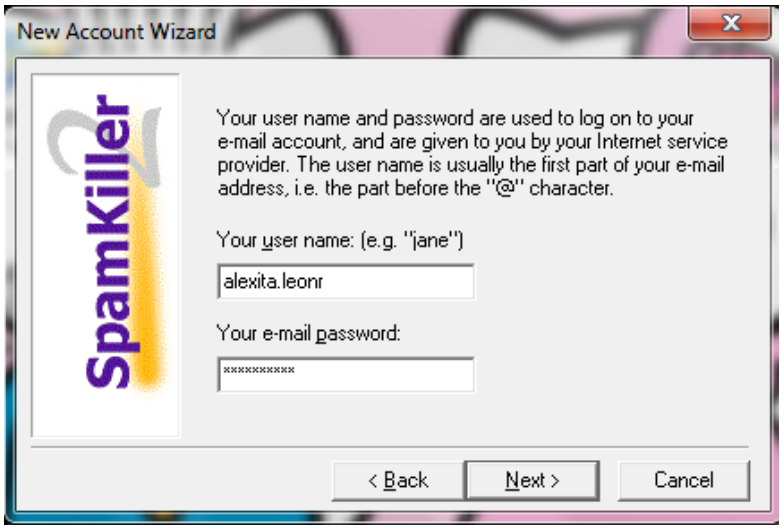
En este paso seleccionamos la cuenta de correo que queremos importar:



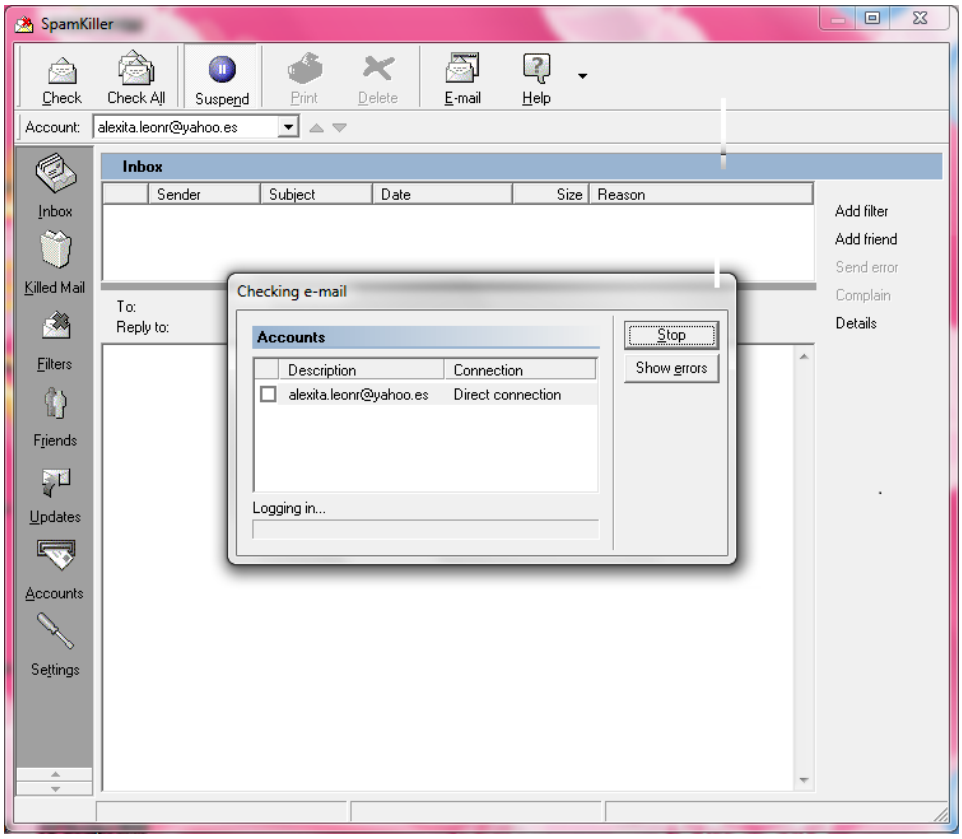
Introducimos nuestro correo electrónico:



Introducimos la contraseña de nuestro correo electrónico:



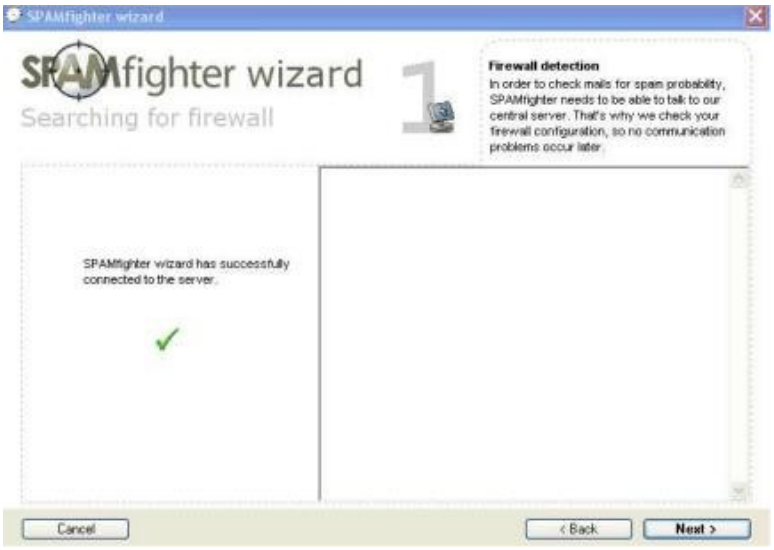
El resultado será algo así:



ANEXO 3: MANUAL DE INSTALACIÓN Y FUNCIONAMIENTO DE SPAMFIGHTER:

El programa es totalmente gratis y esta certificado por Microsoft para todas las versiones de Windows, también existe una versión Pro por la que hay que pagar, pero para un usuario normal con la versión gratuita es suficiente como comienzo.La instalación del programa es muy sencilla, una vez que lo hemos instalado tenemos que registrarnos para activarlo y nos aparecen una serie de ventanas. En esta primera pantalla solo tenemos que dar click sobre **Next**

En la siguiente ventana nos indica que se ha conectado correctamente al servidor y volvemos a dar click sobre **Next**



Si es la primera vez que instalamos el filtro, en la ventana que vemos a continuación seleccionamos la opción **Quiero abrir una cuenta** y volvemos a dar click sobre **Next**

Introducimos nuestra dirección de correo electrónico en la siguiente ventana y ponemos una contraseña para que en caso de algún problema nos reconozcan como usuarios, volvemos a dar click sobre **Next**

A continuación esa información se envía al servidor y tardará unos segundos en actualizarse, cuando acabe, volvemos a dar click sobre **Next** y el programa estará listo

Ahora que ya tenemos instalado y estamos registrados vamos a configurar el programa a nuestro gusto, para ello nos vamos a **Inicio>Programas>SPAMFighter** y damos click en **Configuración**.

En la pestaña de **Opciones** seleccionamos nuestro cliente de correo, el idioma del programa y nos vamos a **Ajustes Avanzados** nos aparece otra ventana como la que vemos en la parte inferior derecha.

En la pestaña **Lista Negra** nos permite agregar manualmente alguna dirección de correo a la lista para que sea bloqueada automáticamente. En la pestaña **Lista Blanca** aparecerán todos los contactos de nuestra lista de correo, podemos pasar alguno a la lista negra si no nos interesa recibir nada de él o bien agregar a la lista blanca alguna cuenta que el programa considera como Spam, pero que nosotros deseamos recibir correo de esa dirección.

En la pestaña de **Language** tenemos la opción de decidir los idiomas de los correos que deseamos recibir. Si marcamos **I only want to receive mail in these lenguages** solamente recibiremos correos en los idiomas que tengamos marcados en la parte inferior.

En la pestaña de **Estadística** veremos un detalle de las acciones que realiza el programa con los correos que recibimos.

Al instalar este programa se integra automáticamente con el Outlook Express, al abrirlo veremos una nueva barra similar a la imagen, desde esta barra podemos realizar algunas acciones sin necesidad de abrir el programa, como Bloquear, Liberar remitentes de correo y también en Mas podemos abril el panel de configuración del programa

Es un programa sencillo de instalar y usar, y aunque no sea espectacular, es gratis, está en español y hace su función.

ANEXO 4: ENCUESTAS