MEDIDAS CONTRA CORREO-ELECTRÓNICO-BASURA (SPAM) EN LA U.A.M.

1. SPAM: correo –electrónico-basura.

Es correo electrónico de naturaleza comercial o publicitaria, en algunos casos ilegal, enviado masivamente a receptores que no lo han solicitado expresamente.

El spam supone un grave problema para el correo electrónico, aproximadamente el 75% de los mensajes que se reciben en la U. A. M. son basura. En el último año se ha pasado de 20.000 a 100.000 mensajes por día.

El incremento en el número de mensajes y la recepción de muchos de ellos en un breve espacio de tiempo hace que el servicio de correo se colapse en determinados momentos.

Los mensajes no solicitados originan una degradación en la calidad del servicio, se demora la entrega de mensajes importantes, debido a la cantidad de mensajes basura que han llegado antes y están en la cola.

El correo vía web, muy útil para el acceso de los usuarios desde cualquier lugar, deja de ser efectivo, ya que el acceso desde conexiones lentas o caras cuando se tiene gran cantidad de correo no deseado, se hace inviable o al menos muy incomodo y puede que caro.

El usuario de correo electrónico tiene la sensación de que el servicio le es poco útil, por el tiempo que pierde borrando mensajes no deseados y, en estos borrados, con frecuencia por equivocación, pierde mensajes válidos.

El spam se recibe por la facilidad que existe para conseguir direcciones de correo válidas. Se utilizan programas que buscan en los webs, en los foros y en los chats estas direcciones. Hay empresas que venden estas direcciones y se pueden comprar por Internet CD´s muy baratos con direcciones válidas.

Los emisores de spam usan diccionarios, combinando nombres y apellidos para mandar mensajes, con lo que consiguen enviar su publicidad y atacar los servidores de correo que son incapaces de atender más de un determinado número de mensajes por segundo.

Cada vez hay más virus que a través de la red infectan PC´s con programas emisores de spam. Estos programas utilizan las direcciones del correo almacenados en el PC y mandan millones de mensajes. En el último trimestre hemos tenido media docena de PC´s infectados en la red de la U.A.M., colapsando durante horas el correo.

2. Medidas posibles contra el fenómeno SPAM.

2.1. En EE.UU. se han aprobado recientemente leyes muy estrictas contra los emisores de spam, con resultado realmente importante.

Se basan en situar fuera de la ley a los emisores de mensajes sin identificación por origen y tema.

2.2. En España no hay legislación específica contra el spam.

2.3. En estos momentos no existe una solución técnica ni legislativa al spam, únicamente se puede paliar el problema. A continuación se describen unas cuantas soluciones técnicas para ello:

2.4. Dificultar la consecución de direcciones de correo.

Para dificultar la consecución de direcciones de correo, hay que evitar publicarlas en el web, en foros de discusión, o en web que no son de confianza, para estos casos se puede usar una dirección de un buzón gratuito. Tampoco hay que responder a los mensajes de spam que dicen que te puedes borrar de su lista si no quieres recibir más mensajes, es una técnica para comprobar que la dirección a la que han enviado el spam es correcta.

2.5. Usar el antivirus institucional y la actualización de sistemas operativos, algunas de ellas automáticas como es el caso de Microsoft.

2.6. Uso de listas negras

Son listas con bases de datos de emisores de spam, siempre se han usado en la U.A.M., rechazan un 10% de mensajes. Hay muchas organizaciones que confeccionan estas listas con diferentes criterios, muchas son sin ánimo de lucro y otras son comerciales.

Inconvenientes:
En algunas ocasiones no están claros los criterios de alta o baja en la lista.

Posible rechazo de mensajes válidos, sin otra alternativa que dejar de usar la lista.

2.7. Uso de listas blancas

Sólo se pueden recibir mensajes desde direcciones que están en una Base de Datos.

Este método es inviable en nuestra institución debido al colectivo de usuarios tan diverso que tenemos en la U.A.M.

2.8. Programas de análisis de contenidos

Los hay de diversos tipos, se usan técnicas para el aprendizaje de lo que es spam y lo que no lo es, baremando las probabilidades de que un mensaje sea basura.

Estos programas son los que más éxito tienen pues frenan los mensajes no deseados y funcionan de dos formas:

- Primera. Etiquetando como SPAM los mensajes que el programa "decide" que lo son y enviándolos al usuario para que los trate convenientemente.

  Ventajas: No hay ninguna pérdida de mensajes y el usuario decide lo que quiere hacer con ellos.

  Inconvenientes: El usuario sigue recibiendo mensajes no deseados aunque convenientemente etiquetados, de esta forma las máquinas siguen procesando todos los mensajes para etiquetarlos y después entregárselos al destinatario, por lo que los colapsos del servicio continúan.

- Segunda. Borrando los mensajes antes de entregarlos usando un criterio basado en el baremo.

Ventajas: Elimina el spam nada más llegar con lo que el usuario no es molestado y no se consumen tantos recursos.

Inconvenientes: Puede eliminar algún mensaje válido, pero en cuanto se detecta se puede corregir el criterio de borrado.
Posibles molestias cuando un usuario no recibe un mensaje que espera.

Se estima que la posibilidad de borrar mensajes válidos, una vez que se ha optimizado el programa es de 1 por cada 100.000, según los diseñadores del mismo.

3. Medidas de Tecnologías de la Información para la U.A.M.

3.1. La entrega de correo-electrónico es uno de los asuntos más serios y estrictos de Tecnologías de la Información y, por tanto, la sola posibilidad de que usando un algoritmo de borrado automático nos hubiera llevado a la pérdida de algún correo nos indica que este asunto excede a nuestro ámbito de competencias y, por tanto, proponemos la mejor solución a fecha de hoy, según nuestro punto de vista.

3.2. Adoptar medidas para dificultar la obtención de direcciones personales de correo de la U.A.M.

3.3. Uso de antivirus y automatización de las actualizaciones del software en los PC´s de la U.A.M. Información al usuario sobre sus ventajas, como hacerlo y posibles penalizaciones

3.4. Uso de un programa de análisis de contenido de la siguiente forma:

1ª FASE: Etiquetación de mensajes como spam e información a los usuarios del uso de filtros y de lo que hace el programa. Optimización de los criterios del programa.

2ª FASE: Valoración del funcionamiento del programa (número de mensajes mal etiquetados).

3ª Fase: Una vez comprobado el buen funcionamiento del programa, borrado de mensajes que sean de spam sin distribuirlos al usuario.

3.5. La primera norma de seguridad informática es no divulgar las medidas tomadas al respecto. Por ello, solicitamos que se deleguen posibles medidas de seguridad informática y telemática en Tecnologías de la Información, que por su automatización no violen la intimidad de las personas, que vayan en beneficio de la comunidad y sean vigiladas por el Vicerrector de Infraestructura y Promoción Tecnológica.