GUIAS DE SEGURIDAD UJA

Correo electrónico no solicitado (SPAM)

1. ¿Qué es el SPAM?

Se define como SPAM o correo basura al conjunto de mensajes publicitarios que son enviados de forma masiva a un número elevado de usuarios al mismo tiempo, sin ser solicitados y que perjudican o interfieren con el resto de mensajes recibidos. Generalmente son recibidos por correo electrónico, pero también a través de otros medios, como el teléfono, la mensajería electrónica o actualmente las redes sociales.

El SPAM presenta una serie de elementos característicos:

- Generalmente tienen un contenido publicitario.
- Suelen tener asuntos llamativos, para captar la atención del destinatario.
- La dirección del remitente suele ser desconocida e incluso en muchos casos falsificada.

2. Técnicas usadas por los spammers

El principal objetivo de los spammers es el de conseguir el mayor número de direcciones de correo válidas y operativas. Para ello, utilizan numerosas y variadas técnicas:

- **Uso de listas de correo:** los spammers se dan de alta en numerosas listas de correo y consiguen las direcciones de correo electrónico de todos los usuarios pertenecientes a cada una de esas listas.

- **Uso de programas específicos de rastreo automático** que recorren Internet en busca de direcciones de correo a partir de numerosas fuentes (páginas web, grupos de noticias, blogs, etc).

- A partir de la **compra de extensas bases de datos de**

direcciones de correo comercializadas por particulares o empresas.

- **Generación de direcciones de correo artificiales a partir de un dominio de Internet**, cambiando el nombre de usuario y enviando mensajes a las mismas. Así, los spammers averiguan cuáles de las direcciones generadas son reales, usando diccionarios de palabras o directamente mediante fuerza bruta, probando numerosas combinaciones de letras y números de forma automática.

- A partir de **correos electrónicos con chistes, cadenas y adjuntos** que se suelen reenviar sin ocultar las direcciones (sin usar el campo Bcc), y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o por un usuario malicioso.

- **Hoaxes**. Son mensajes de correo electrónico, generalmente distribuidos en cadena, con contenido falso o engañoso. Algunos de estos mensajes están relacionados con virus falsos, fórmulas para ganar rápidamente una enorme cantidad de dinero, falsos mensajes de solidaridad y timos de lo más variado.

- A partir de la entrada ilegal en servidores lo que permite descargar cuentas de correo electrónico, una vez comprometidos los servidores.

- **Mediante troyanos y ordenadores zombis pertenecientes a botnets**. Últimamente se ha extendido el uso de una técnica consistente en la creación de virus y troyanos que se expanden masivamente por ordenadores que no están protegidos adecuadamente. Estos ordenadores infectados son utilizados por los spammers como "ordenadores zombi", que envían correo basura a sus órdenes, pudiendo incluso rastrear los discos duros o clientes de correo en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora que esta infectado (no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que se le deniegue el acceso a determinadas páginas o servicios. Actualmente, se calcula que el 40% de los mensajes no deseados se envían de esta forma.

- **Servidores de correo mal configurados**. En concreto los servidores configurados como open relays (reencaminadores abiertos) no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos, por lo que cualquier puede hacer uso de ellos para el envío. Existen diferentes bases de datos públicas que almacenan listas de servidores configurados como open relays que permiten que los spammers hagan uso de ellos.

3. Cómo combatir el SPAM. Medidas prácticas

- **Desconfiar de los correos de remitentes desconocidos**. Ante la duda, eliminarlos directamente.

- **No abrir ficheros adjuntos sospechosos** procedentes de desconocidos o que no hayamos solicitado. **En cualquier caso, analizar los adjuntos con un buen antivirus** antes de ejecutarlos en nuestro sistema.

- **Utilizar el filtro anti-spam** de nuestro cliente de correo electrónico y marcar los correos como correo basura aquellos que estamos seguros que lo son, para entrenar al filtro y mejorar la detección en el futuro.

- **Oculta tu dirección de correo electrónico**, publicando un nombre y dirección falsos. Por ejemplo, podríamos renombrar la cuenta

  usuario@ejemplo.com

  como

  usuarioNOS@PAM.ejemplo.com

  Cualquiera podría enviarnos correo sustituyendo la parte NOS@PAM por @, pero para un spammer sería una dirección no válida.

  También puedes usar una imagen para publicar tu dirección de correo electrónico, en lugar de escribirla directamente.

- **No respondas nunca al SPAM**. Los spammers solicitan a menudo respuestas a sus mensajes y usan cualquier respuesta del destinatario como confirmación de que una dirección de correo electrónico es válida. Igualmente, muchos mensajes de SPAM contienen enlaces o direcciones que aparentemente permiten al usuario ser eliminado de la lista de correo de SPAM. En la gran mayoría de los casos estos enlaces no conducen a la dirección del destinatario, sino que conducen a más SPAM.

- **Sé prudente al rellenar formularios en páginas web.** Los formularios permiten a los usuarios enviar su correo electrónico, entre otros datos, mediante un simple navegador web. En muchos casos, no podemos ver la dirección de correo electrónico destino a la que se envían los datos, por lo que resultan una forma habitual de captar direcciones de correo electrónico. **Esta recomendación es especialmente importante si nos solicitan contraseñas, números de tarjeta de crédito o cualquier otra información sensible.**

- **Desactiva el HTML en el correo electrónico** siempre que sea posible. El formato HTML puede generar un amplio conjunto de amenazas. Si desactivamos en nuestro cliente de correo electrónico la vista previa de los mensajes, la descarga automática de imágenes y otros elementos y no usamos HTML, imágenes o archivos adjuntos en nuestros mensajes, tenemos mucho menos riesgo de recibir SPAM y evitaremos cualquier posible código malicioso que pueda estar incluido en el cuerpo de los mensajes.

- **Es aconsejable disponer de direcciones de correo electrónico alternativas** para usarlas en casos puntuales donde tengas que facilitar tu dirección de correo electrónico sin tener la garantía absoluta de que el sitio no enviará SPAM, asegurando así nuestra dirección de correo habitual.

- Ten precaución con los **mecanismos de recuperación de contraseñas que ofrecen muchos sitios webs.** Generalmente proponen elegir una pregunta que le harán al usuario en caso de que solicite recuperar su contraseña. En estos casos, se recomienda utilizar una pregunta cuya respuesta sólo conozcamos nosotros.

- **No facilites tu cuenta de correo a desconocidos** ni la publiques alegremente en Internet.

- Cuando reenvíes mensajes a múltiples destinatarios **utiliza siempre la copia oculta** (CCO ó BCC) para introducir las direcciones de los destinatarios.

4. Referencias en Internet

- Instituto Nacional de Ciberseguridad (INCIBE)
  http://www.incibe.es/
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- RedIris – Abuso en el servicio de correo electrónico
  http://www.rediris.es/mail/abuso/
- http://www.delitosinformaticos.com/