Una gran cantidad de los reportes recibidos en la Línea de Denuncia de ASI corresponden a correos no solicitados, comúnmente conocidos como correo basura o SPAM. Es por ello que hemos preparado este artículo que ofrece una explicación de los tipos de correos que hemos recibido para que estés alerta y no caigas en engaños, ya que en la mayoría de los casos el SPAM es un vehículo para diferentes calamidades digitales que debemos aprender a evitar.

Origen del término SPAM.

Es curioso que originalmente el término SPAM no tenía nada que ver con el correo electrónico. En 1937 la empresa Hornel Foods lanzo una carne enlatada llamada "Hornel's Spiced Ham". El gran éxito de este producto se basó en que la lata incluía un mecanismo de apertura que libraba al consumidor de la necesidad de usar un abrelatas y no requería refrigeración. Su popularidad logro que el nombre se volviera genérico, así como hoy en día a cualquier pañuelo desechable le llamamos "Kleenex", SPAM es un acrónimo para Spiced Ham.

Más adelante el grupo británico Monty Phyton hizo burla del producto que ya se encontraba en todas partes. En un sketch cómico presentaron a un grupo de vikingos tratando de comer en una taberna, cuya propietaria les recitaba el menú, que incluía Huevos con spam, tocino con spam, salchichas con spam, spam con spam, spam, spam, spam! Al final los vikingos cantan alegremente repitiendo el término a coro.

Alrededor de 1970, el termino SPAM ya se usaba en Inglaterra y en EUA para referirse a cualquier cosa que fuera abundante. Por esas fechas el consumidor se empezó a cansar del producto, e incluso hubo campañas para desprestigiarlo ya que teóricamente era malo para la salud, con lo que el término SPAM se empezó a aplicar a cosas abundantes y no deseadas, lo que explica muy bien por qué le queda perfectamente al molesto correo no solicitado.

Tipos de SPAM

Hemos recibido reportes de SPAM en:

a) Correo electrónico
b) Mensajería instantánea (también llamado SPIM)
c) Foros
d) Blogs
e) Teléfonos móviles
f) Grupos de noticias.

Sin embargo, por su abundancia y mayor potencial de impacto negativo, nos referiremos al SPAM en correo electrónico, aunque como se verá, muchos de los conceptos, sobre todo de prevención, aplican en cualquier tecnología.

Temas de SPAM en el correo electrónico.

En cualquier caso estamos hablando de correos que nos ofrecen información que puede o no interesarnos, pero que nosotros NO SOLICITAMOS.

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.

Si bien hay ocasiones en que el correo contiene simple información comercial de productos o servicios y solo son una molestia constante saturando nuestro buzón de entrada (como es el caso de las molestas cadenas), en la mayoría de los casos incluyen tecnología que puede desde modificar nuestro navegador para que siempre abra una página comercial, hasta causar daño al equipo, información o al patrimonio del usuario, por lo que es importante la precaución.

A nivel mundial los temas más recurrentes en el SPAM y son: (con ejemplos de los asuntos)

- Pornografía
  Compre una web-cam y quiero que me veas desnuda!
  Satisface a tu pareja

- Salud
  Baja de peso en una semana!
  Compra Valium a precio de mayoreo

- Piratería
  Ofrecemos licencias OEM al 10% de su valor
  No pagues precios de lista, tenemos grandes ofertas en marcas comerciales

- Educación
  Consigue tu diploma universitario
  Gradúate desde tu casa, precios accesibles

En México, los temas más comúnmente reportados en ASI son:

- **Cadenas.**
  Te piden que le avises a todos tus contactos sobre nuevos virus, oraciones por la paz, etc…
- **Fraude Nigeriano.**
  Te escribe un supuesto funcionario bancario corrupto de algún país lejano (normalmente africano o del este de Europa) que busca sacar grandes cantidades de dinero con tu ayuda ofreciéndote una jugosa comisión. Pueden hacerte creer que ganaste una lotería, eres el beneficiario de una herencia, etc… Este es uno de los temas de engaño con más reportes, sobre el **te recomendamos mucho que revises nuestro artículo "El fraude Nigeriano en internet".**
- **Newsletter que no ofrecen mecanismos de desuscripción.**
  También llamado Opt-out, todo newsletter debe ofrecer al usuario un mecanismo para dejar de recibir los correos. Si no lo tiene, o bien, si pides la cancelación y no te hacen caso, debes reportarlo en Profeco.
- **Ofertas de Pornografía gratuita.**
- **Ofertas de trabajo falsas.**
  Personas que enviaron sus datos completos y curriculum en una solicitud de trabajo, pero son contactados por alguien externo quien les ofrece asignarles el puesto a cambio de dinero.
- **Phishing bancario.**
  El usuario recibe un mensaje supuestamente desde su banco en que se le informa que por

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.

diferentes razones es necesario que actualice sus datos completos, y ofrecen ligas que te llevan a portales igualmente falsos que intentan robar tu información confidencial.

- **Tarjetas Postales falsas.**
  Clásico mensaje que dice "un amigo te ha enviado una postal", ahora usan nombres comunes para tratar de engañarte, por ejemplo "Manuel te ha enviado una postal", buscando la posibilidad de que conozcas a alguien que se llame Manuel.
- **Recargas de tiempo aire.**
  Sin duda, el tema más frecuente con el que se busca engañar al usuario, ofreciendo el doble o triple de tiempo aire siguiendo ligas o instrucciones falsas. **Sobre este tema te recomendamos mucho que revises nuestro artículo "Las imágenes del fraude".**
- **Robo de contraseñas.**
  Muy difundido entre los jóvenes, son mensajes que te ofrecen darte a conocer quién te ha borrado de su mensajería instantánea, pero te piden tu nombre de usuario y contraseña y comúnmente la conservan para mandar mensajes en tu nombre a terceros.
- **Diversos.**
  Es la última vez que te molesto, ¿Ya te olvidaste de mi?, Mensajes que llegan como si vinieran de tu misma cuenta de correo, Piratería, Invitaciones a cursos, Servicios de asesorías, etc…

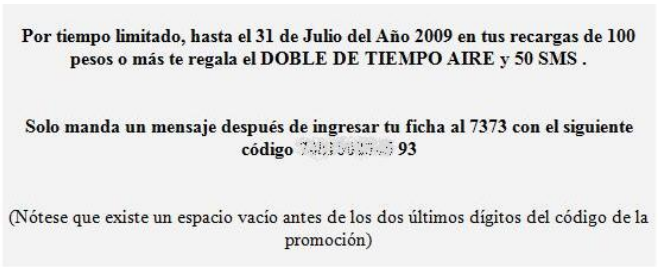
¿Cómo puede causarme daño un correo electrónico?

Además de la constante molestia que implica recibir decenas y hasta cientos de correos basura por semana, en la mayoría de los casos mencionados arriba, los defraudadores que envían los correos buscan el lucro por medio de la estafa, intentan engañarnos para lograr obtener nuestro dinero o nuestra información confidencial para después hacer mal uso de ella, casi siempre con daño a nuestro patrimonio.

¿Cómo lo logran? A continuación presentamos las categorías de los casos recibidos en ASI a la fecha:

a) **Ingeniería social.**

No hacen uso de complicados mecanismos o tecnología para obtener tu información o patrimonio, pero logran engañarte para que tú mismo lo entregues. El ejemplo más ilustrativo es el de la oferta de duplicar tu tiempo aire enviando un código por SMS al 7373 después de abonar una tarjeta de 100 pesos.



La verdad es que así es como se transfiere saldo de un celular a otro, pero muchos usuarios desconocen esto. **Sobre este tema te recomendamos revisar el artículo "Las imágenes del Fraude**". Los usuarios que reciben un correo como el de la imagen, y envían el código solicitado, en realidad transfieren $93 pesos de su propio saldo al número XXXXXXXXXX, que por supuesto cambia frecuentemente. (XXXXX…. es un número de teléfono móvil)

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.

b) Archivos adjuntos contaminados.

El mensaje puede venir acompañado con archivos que contengan virus o código malicioso (malware). Si el usuario intenta abrirlos, su equipo se contamina automáticamente, a menos que cuente con la protección actualizada.

Un ejemplo de lo anterior fue una serie de correos falsos que decían provenir de "Profeco Informa", y engañaban al usuario diciendo que se acompañaba un archivo con la lista de las gasolineras donde se ofrecían litros completos de gasolina, pero que en realidad contenían Malware para espiar al usuario. (Ver más adelante "¿Cómo me puede afectar el Malware?")

c) Redirección a páginas falsas.

Con cualquier pretexto, un correo electrónico puede tratar de engañar al usuario para lograr que visite una página fraudulenta. Al momento de visitarla, la página puede intentar sembrar código malicioso (malware) en el equipo, o bien, presenta un formulario solicitando información confidencial del usuario, como nombre completo, dirección y números de tarjetas de crédito.

Un engaño muy común en estas páginas es que presentan un mensaje informando al usuario que "para visualizar la página se requiere instalar la última versión de Adobe Flash player" y pide permiso para instalarlo (como si fuera muy legal). La realidad es que la aplicación intentaría sembrar código malicioso en el equipo.

El caso más común de este tipo de engaños es el conocido como "Phishing Bancario", en donde el usuario recibe un correo con un texto similar a:

> Banequis le informa que es necesario sincronizar su dispositivo de acceso seguro, para realizar esto:
>
> Fírmese en su cuenta y el sistema sincronizara sus claves automáticamente.
>
> **Para Personas**
>
> 
>
> **Para Empresas**
>
> 

Si el usuario hace clic sobre la imagen de "Para Personas" o "Para Empresas", es redirigido a una página que intentará sembrar código malicioso o solicitará información confidencial.

Si bien el primer caso utiliza Ingeniería Social pura, en los dos restantes también se utiliza para manejar historias convincentes que engañen al usuario para lograr que abra los archivos adjuntos o que visite la página fraudulenta.

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.

¿Cómo me puede afectar el Malware si llega a mi computadora?

Como mencionamos antes, el SPAM es un vehículo para conducir código malicioso (malware) hasta tu computadora. Como se vio en los ejemplos mostrados, varios de los esquemas de engaño buscan sembrar Malware para diferentes propósitos, aquí te presentamos los más comunes para que comprendas la importancia de mantener tu equipo protegido por software de seguridad:

Spyware
Puede espiar y guardar registro de los sitios que visitas para informarlo al creador del código sin que te des cuenta.

Virus, Troyanos y Gusanos
Que pueden utilizar tu máquina en centro de envío de correos basura (Spammers) o utilizarla para atacar a otros usuarios o sitios de internet (**a esto se le llama convertirla en "Bot" o Zombie**), localizar información confidencial en tu equipo, e incluso, destruir información irremediablemente.

Backdoors
Abre un puerto de tu equipo para que el autor del malware pueda controlarlo, instalarle otros códigos, usar los recursos del equipo, etc…

Dialers
Hacen llamadas a números de paga con cargo al recibo del usuario, esto solo aplica en conexiones dial-up

Keyloggers
Registran todo lo que se escribe en el teclado de la computadora, almacenándolo en archivos ocultos que después son enviados al autor del Malware. Esto puede incluir desde nombres de usuario, contraseñas, números de cuenta, o incluso hasta correos y documentos personales, es decir, todo lo que el usuario escriba.

No es difícil imaginar el mal uso de tu propia información una vez que el autor del Malware la recibe por cualquiera de estos métodos. Existen muchos otros tipos, sin embargo estos son los más comunes si te interesa conocer información de otras variantes también peligrosas, te invitamos a consultar el siguiente artículo en Wikipedia:

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

Donde te explican lo que es el Adware, Exploits, Hoaxes, Rootkits, etc…

Además, te invitamos a revisar estos otros contenidos de nuestra biblioteca:
¿Es delito el SPAM en México?
Correos engañosos
El Fraude Nigeriano en Internet
¿Cómo me localiza un Spammer?

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.

PREVENCIÓN.

La medida más relevante para prevenir el SPAM es activar el filtro anti-spam de tu programa de correo electrónico, como Mac Mail, Outlook, etc…

Estos filtros se encargan de revisar aspectos técnicos de los correos que reciben para determinar si son válidos o no. Si determinan que son correos no solicitados o SPAM, los envían a un buzón de correo basura.

Ejemplos de aspectos técnicos a revisar son: demasiadas palabras como "gratis", "free", etc… en el asunto o en el mensaje, imágenes con ligas, discrepancias entre la dirección del remitente y el valor en "Responder a:", etc…

Es importante mencionar que estos filtros no son infalibles, por lo que la precaución debe persistir, y en un número mínimo de ocasiones, un correo válido puede ser depositado en el buzón de correo basura, por lo que es conveniente revisarlo de vez en cuando.

Existen muchas formas en que los "spammers" pueden conseguir lotes de correos electrónicos en donde fácilmente puede estar incluida la tuya, no dejes de revisar el artículo ¿Cómo me localiza un Spammer?.

Recuerda que si tienes dudas, puedes reportar cualquier correo en la Línea de Denuncia de A.S.I. p ponerte en contacto con nosotros para cualquier aclaración.

Staff A.S.I.

Ayúdanos a que esta iniciativa crezca, te invitamos a promover nuestras secciones:

DENUNCIA.
Páginas web, correos electrónicos y foros o chats con **contenido ilegal o fraudulento** pueden ser reportados aquí para su dictamen e informe a las autoridades correspondientes.

CENETIC.
Participa en encuestas que nos permiten comprender tus puntos de vista.

BLOG.
Participa en las discusiones abiertas, tu opinión vale!

VIDEOS.
Revisa la mejor recopilación de videos educativos sobre seguridad en internet.

CORRE LA VOZ.
¡Tú puedes ayudarnos a tener un Internet más limpio!
En esta sección puedes encontrar banners descargables para colocar en blogs o páginas web, y apuntarlos a nuestro sitio.

DONATIVOS.
Podemos realizar muchas actividades con los fondos que recibimos por medio de donativos deducibles de impuestos. Si tú, tu organización o alguien que conoces puede apoyar a esta A.C., **de antemano te damos las gracias por invitarlos a que conozcan esta sección.**

© D.R. Alianza por la Seguridad en Internet A.C. www.asi-mexico.org
Este contenido llega a ti por una cortesía de los miembros de A.S.I. para tu consulta personal únicamente. Prohibida su reproducción parcial o total por cualquier medio sin nuestra autorización previa por escrito.