Con el reciente incremento en el volumen de correo no solicitado (SPAM) que por diversas razones logra pasar los filtros anti-spam de los usuarios, y sobre todo, por la creciente creatividad en el uso de Ingeniería Social por parte de los creadores de estos molestos pero muchas veces creíbles mensajes, la Línea de Denuncia de ASI ha recibido repetidamente la siguiente pregunta:

Si yo no le doy mi dirección casi a nadie, ¿Cómo es que un spammer puede encontrarme, y empezar a mandarme cientos de correos basura?

No hay una respuesta sencilla a este planteamiento, por lo que hemos creado este contenido que explica solo las formas más comunes en que tu dirección de correo puede caer en manos de un spammer, con la intención de enfatizar lo importante que resulta que aprendas a mantenerte apartado de esta calamidad, o en su momento, de ser engañado.

¡No caigas en el engaño!

Se conocen como **Spammers** a aquellos que mandan correo electrónico basura o no solicitado para promover productos o servicios. **No te están buscando a ti**, están buscando a un millón de personas como tú. Su meta es contactar a la mayor cantidad de gente en línea como les sea posible para que puedan generar el mayor número de respuestas posibles.

Los niños están especialmente en riesgo ya que tienen menos precaución al utilizar servicios en internet y se comunican más comúnmente en salas de Chat con desconocidos.

Los Spammers te pueden encontrar de muchas maneras, incluyendo:

Los perfiles públicos o semi-públicos y las páginas blancas y amarillas en línea.
Hay una gran variedad de sitios web que permiten a los miembros crear perfiles y buscar miembros con perfiles similares, como es el caso de las redes sociales (Hi5, Facebook, etc…). Los spammers utilizan estos sitios para recolectar direcciones de correo electrónico de acuerdo con ciertos intereses. Otros sitios sirven como buscadores de personas o negocios en la web. Las páginas blancas y amarillas contienen direcciones de varias fuentes que frecuentemente comparten contactos.

Salas de Chat.
Los Spammers recolectan nombres en las Salas de Chat, ya que esto les permite “dirigir” sus listas de correo.

Páginas Web.
Los Spammers tienen programas que “olfatean” a través de las páginas web para inspeccionarlas buscando direcciones de correo electrónico. Algunos sitios solicitan varios detalles a través de formatos (por ejemplo, libros de visitas y formatos de registro). Los spammers pueden conseguir direcciones de correo electrónico a través de éstos, ya sea porque el formato está disponible en la red o porque el sitio vende/da la lista de correos electrónicos a otros.

Tu propio navegador.
Algunos sitios utilizan varios trucos para extraer la dirección de correo electrónico de tu navegador web (Firefox, Chrome, Internet Explorer, etc…), algunas veces sin que te des cuenta. Un ejemplo es hacer que el navegador web extraiga una de las imágenes de la página a través de una conexión anónima al sitio. Para poder accesar la página, algunos navegadores web ofrecen la dirección de correo electrónico que el usuario configuró en el navegador como la contraseña para esa cuenta.

Cadenas y engaños (hoaxes).
Este método significa que los spammers utilizan un **hoax** (trampa) para convencer a la gente que les den direcciones de correo electrónico válidas. Por ejemplo, algunos spammers utilizan cadenas con promesas de regalos gratuitos para ti y cualquiera a quién se le reenvíe la cadena siempre y cuando se le copie al spammer. Comúnmente fingen estar asociados con negocios grandes de buena reputación.

Grupos de Noticias.
Los spammers regularmente exploran grupos de noticias para conseguir direcciones de correo electrónico utilizando programas diseñados para extraer las direcciones de cualquiera que sea un miembro de ese grupo de noticias.

Listas de correos.
Los spammers regularmente intentan obtener listas de suscriptores a listas de correos porque algunos servidores de correos (mail servers) los entregan a los que lo soliciten.

Protocolos no protegidos.
Existen diferentes aplicaciones y protocolos (conjuntos de reglas) en los servidores de correos que deben estar ben protegidos por su administrador para evitar que usuarios mal intencionados se conecten y extraigan información de cuentas de correo sin autorización. Ejemplos son el protocolo Finger, Ident, Telnet, etc…

Puntos de contacto de un dominio.
Cada domino tiene de uno a tres puntos de contacto típicos cuyas direcciones son fácilmente adivinadas por los spammers, por ejemplo admin@tudominio.com, webmaster@tudominio.com y contacto@tudominio.com

Archivos de identificación (Cookies)

Además de extraer las direcciones de correo electrónico de los sitios web utilizando los métodos arriba mencionados, muchos sitios web y utilizan "cookies" para monitorear cada uno de tus movimientos en sus sitios.

Un cookie es un identificador único que un servidor web coloca en tu computadora. Es un número de serie personal para ti que puede ser utilizado para recuperar tus registros de su base de datos, por ejemplo de visitas anteriores, que secciones visitaste, etc…

Normalmente, es una cadena de letras al azar que es lo suficientemente larga para ser única. Éstas se guardan en un archivo en una carpeta de tu equipo.

Las cookies pueden aprender tus preferencias y esa información puede ser utilizada como la base para ofrecerte o no ofrecerte información en futuras visitas. Las Cookies pueden ser utilizadas para rastrear donde navegas en un sitio, qué escoges en respuesta a las opciones que se te ofrecen al navegar en él, etc…

Cualquier sitio web que conoce tu identidad y tiene un cookie para ti podría instalar los procedimientos para intercambiar la información que tienen de ti con otras compañías que adquieren espacios de publicidad con ellos, y de esta manera sincronizar las cookies que ambos tienen en tu computadora.

Esta posibilidad significa que una vez que tu identidad se vuelve conocida para una sola compañía enlistada en tus cookies, cualquiera de las otras compañías podría saber quién eres tú cada vez que visites sus sitios.

El resultado es que si un niño entra a un sitio de pornografía aunque sea ligera y se registra para ganar un viaje o cualquier otro "premio", el nombre y datos de ese niño puede ser vendido tanto a otros sitios web de pornografía incluso extrema, como a agencias de viajes, venta de farmacéuticos, etc…

Existen muchos usos convenientes y legítimos de las cookies.
Por ejemplo, permiten que haya "personalización masiva" del contenido de un sitio web para que solo veas lo que realmente puede interesarte. Además, no pueden pasar un virus a tu equipo. La información contenida en las cookies no es un programa y nunca es ejecutada como un código, y por lo tanto no pueden realizar acciones como tomar información de tu disco duro, de la configuración de tu equipo, números de tarjetas de crédito, etc…

Tampoco pueden captar tu información personal, a menos que des voluntariamente esta información en un sitio, por ejemplo, en respuesta a una oferta de algún tipo. Si tú si das esa información voluntariamente, esa información podría aparecer en una cookie y puede ser utilizada en intercambios con otras empresas

Existen recursos de Internet legítimos que pueden ser mal utilizados.
Una vez que alguien tiene tu dirección de correo electrónico, existen recursos legítimos de Internet que pueden ser mal utilizados para encontrar información adicional acerca de ti. Por ejemplo, los spammers pueden llevar a cabo búsquedas en grupos de noticias para revisar si tienes un sitio web, si estás en un sitio web, o si has publicado mensajes en esos grupos de noticias.

PREVENCIÓN.
Es prácticamente imposible "blindar" tu dirección de correo para que no caiga en manos de un spammer, por lo que la sugerencia más generalizada es que utilices una cuenta de correo anónima para participar en foros, registrarte en sitios web, etc… y dejes otra dirección de correo electrónico para mensajes relacionados con tu trabajo o asuntos serios, y nunca la ofrezcas en formularios de sitios como entretenimiento, turismo, etc. SI te das cuenta, el hecho de que un spammer tenga tu dirección de

correo no sería tan grave si esta no se encuentra asociada a datos que puedan identificarte en el mundo real, como tu nombre, dirección postal, etc…

Y por supuesto es recomendable que actives un filtro anti-SPAM en tu equipo. 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.

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.

A la fecha de esta publicación (Agosto 2009), lamentablemente el SPAM no es considerado ilegal en México, sin embargo esto tampoco sería una solución definitiva. En los Estados Unidos, en donde si es ilegal, se genera más del 40% del SPAM mundial, es decir, hablamos de millones de correos, que ninguna autoridad podría realmente contener.

Tenemos mucha información sobre este tema en la sección de contenidos en www.asi-mexico.org/contenidos, te invitamos a consultarla.

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.

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.**

Visita el nuevo sitio www.CivismoDigital.org

Y nuestras redes sociales: