# Grupo de Trabajo Antiabuso de Mensajes, Malware y Móvil (M3AAWG)

# ¡Socorro, M³AAWG! Caí en una trampa de spam

**Febrero de 2023**

La URL de referencia para este documento es: https://www.m3aawg.org/help-i-hit-a-spam-trap

## Introducción

Este documento ayuda a los proveedores de servicios de correo electrónico (ESP) a mitigar las consecuencias de caer en una trampa de spam. También sugiere formas de utilizar la información que proveen estas trampas para mejorar las prácticas de envío de los clientes, minimizando así futuros eventos de spam. En este documento, "cliente" se refiere a la organización que utiliza el ESP para enviar correo electrónico.

La mayoría de los remitentes de correo electrónico se enfrentan en algún momento a las consecuencias de haber enviado mail a una trampa de spam. La magnitud de las consecuencias varía significativamente según la cantidad de mensajes enviados a la trampa, el tipo de trampa, quién la opera y otras variables que los clientes podrían no conocer. En estos casos, los ESP tienen la responsabilidad de monitorear e informar a sus clientes si se produce un evento. El ESP querrá evitar acceder a estas trampas en el futuro y mitigar los efectos de estos eventos en la entrega de correo. No hacerlo podría tener consecuencias más graves en toda su infraestructura de envío de correo.

Una alta tasa de mensajes enviados a una trampa de spam desde un flujo de correo determinado puede indicar un remitente abusivo o, como mínimo, uno que aplica las mejores prácticas de envío de forma inconsistente (los estándares recomendados se describen en M³AAWG Sender Best Common Practices. El dominio del destinatario puede decidir que lo mejor para sus usuarios es rechazar los mensajes de ese flujo o asignar menor prioridad a los correos presentados para su entrega. En circunstancias extremas, el ESP puede descubrir que ha sido bloqueado y que sus correos han sido rechazados por una gran parte de Internet.

Si bien nadie quiere caer en una trampa de spam, el ESP puede aprovechar las visitas a una de estas trampas como una oportunidad no solo para detectar y eliminar a los clientes abusivos, sino también para ayudar a sus clientes legítimos a identificar y corregir las malas prácticas de envío. Más adelante hablaremos sobre mitigación y presentaremos algunos puntos de discusión para compartir con los clientes.

## ¿Qué es una trampa de spam?

Una trampa de spam es una dirección de correo electrónico que se utiliza para recolectar, registrar y

monitorear el envío de spam y otros correos no solicitados o abusivos. Estas trampas están diseñadas para ser indistinguibles de otras direcciones de correo electrónico y pueden encontrarse en todo tipo de redes, incluso en dominios corporativos y de correo gratuito.

Aunque existen diferentes tipos de trampas de spam, todas comparten una característica: no envían mensajes ni se suscriben a listas de correo ni a boletines informativos. El operador de una trampa monitorea los mensajes enviados a esas direcciones y utiliza los datos para analizar la reputación de la dirección IP y el nombre de dominio, y también para evaluar el contenido del correo electrónico.

Muchas veces estos datos se utilizan y redistribuyen a través de listas negras basadas en DNS (DNSBL) y otros sistemas de reputación para ayudar a tomar decisiones informadas sobre entrega o bloqueo en los dominios destinatarios que los utilizan.

## Una taxonomía de las trampas de spam

Los siguientes son algunos de los tipos de trampas más comunes:

**Trampa reciclada**

> Una dirección o dominio que alguna vez fue válido, pero que después de un período de inactividad se convirtió en una trampa de spam. La duración de la inactividad puede variar significativamente entre operadores, pero M[3]AAWG sugiere un mínimo de 12 meses. Caer en una trampa de este tipo suele ser un indicador de una lista mal gestionada (o de una lista antigua) y/o de la falta de un buen procesamiento de los rebotes.

**Trampa prístina o pura**

> Una dirección que nunca estuvo activa para un usuario de correo electrónico antes de su implementación como trampa de spam. En estas trampas se suele caer como resultado de la recolección de datos en la web, el sondeo del espacio de direcciones o ataques de diccionario. Caer en este tipo de trampas puede ser un fuerte indicador de listas compradas.

**Trampa tipográfica**

> Estas trampas típicamente incluyen un error tipográfico intencional y quizás común, con mayor frecuencia en la parte de la dirección correspondiente al dominio, por ejemplo, user@gmial.com, user@notmail.com y similares. Caer en este tipo de trampas suele indicar que el cliente no confirmó la dirección del destinatario, posiblemente como resultado de errores de transcripción o escaneo cuando el remitente la recogió. Si bien técnicamente esto puede considerarse una trampa prístina, muchos operadores las clasifican de forma diferente, ya que los remitentes pueden obtenerlas a través de prácticas de recolección legítimas.

M[3]AAWG Best Current Practices for Building and Operating a Spam Trap (Mejores prácticas actuales para construir y operar una trampa de spam) contiene un desglose más detallado de los tipos de trampas de spam y cómo se usan. Este documento se refiere principalmente a las trampas que afectan directamente la entrega, no a las redes de trampas de sensores que se utilizan para monitorear la reputación en vez de para bloquear el correo.

## Sabes que has caído en una trampa de spam cuando...

Como las trampas de spam suelen estar diseñadas para que no se puedan distinguir de otras direcciones de correo electrónico, muchas veces es difícil saber cuándo un mensaje determinado se ha enviado a una de ellas. Sin embargo, existen indicadores de que estamos enviando mensajes a una trampa de spam, entre ellos, la inclusión de un dominio o una IP en una lista negra o un aumento de la cantidad de correos rechazados. Las herramientas que monitorean las listas negras y la reputación pueden ofrecer métricas sobre los envíos a trampas de spam sin revelar (o "quemar") las trampas de spam en sí.

Excepcionalmente, un dominio destinatario anuncia la existencia de una trampa de spam. Esto puede hacerse a través del nombre de host de su servidor MX en DNS (por ejemplo, spamtrap.domain.com) o mediante un texto en una respuesta SMTP que indique que la dirección es una trampa de spam.

También existen feeds de trampas de spam comerciales. A estos servicios los proporcionan empresas de monitoreo de la entregabilidad y tienen sus propias redes de trampas de spam. Estas redes no se utilizan para bloquear, sino para permitir que los clientes de las empresas que monitorean la entregabilidad vean qué parte de su correo se está enviando a estas trampas.

## Exposición involuntaria de trampas

En general, quienes operan las trampas no buscan exponerlas. Crear y mantener trampas que puedan producir datos útiles requiere de una inversión significativa. Los operadores deben asumir que una vez expuesto, el conocimiento de la existencia de una trampa se difundirá rápidamente, minimizando así su efectividad.

Durante el proceso de investigación y remediación, los ESP o sus representantes pueden revelar sin darse cuenta la identidad de una dirección IP, dominio o red que sea una trampa de spam. Para mantener el funcionamiento discreto requerido, los ESP deben tomar todas las medidas adecuadas para mantener la confidencialidad de estos datos.

**La comunicación con el cliente nunca debe revelar explícita o implícitamente la identidad de las trampas o redes, y cualquier discusión de estos datos por parte de un ESP debe manejarse estrictamente bajo el principio de "necesidad de conocer".**

Si se revelan datos que permitan identificar la trampa o la red y se conoce la identidad de su operador, sería recomendable notificar al operador de la trampa. Informar al operador que su trampa puede estar comprometida le permitirá tomar las medidas necesarias para mantener la efectividad de su red. Además, notificar al operador de la trampa puede ayudar a un ESP a establecer o mantener una relación de trabajo positiva con el propietario de la red.

## Remediación

### Notificar al cliente

Un ESP debe notificar a su cliente cuando hay evidencia de que se ha caído en una trampa de spam. A continuación presentamos algunas consideraciones que se deben tener en cuenta al notificar a un cliente este tipo de eventos.

**Auditoría de adquisición**

En general, los eventos con trampas de spam requieren una auditoría de los procedimientos de adquisición que permitieron que la dirección de la trampa terminara en la base de datos del remitente. Esta auditoría necesariamente se parecerá a los procedimientos de verificación de listas detallados en M[3]AAAWG Vetting Best Common Practices. Sin embargo, algunos de sus aspectos exigirán un enfoque más granular y deberán incluir consideraciones adicionales como las siguientes:

- ¿Cómo se crearon las listas de contactos? Una auditoría del proceso de adquisición debería enfocarse principalmente en los métodos utilizados para adquirir y verificar los destinatarios dentro de cada lista de contactos.
- ¿Es posible saber cuándo el remitente envió por primera vez un mensaje a una trampa de spam y correlacionar ese evento con un envío específico o un segmento de una lista que luego pueda analizarse?
- ¿Apareció la IP o el dominio en una lista de bloqueo como resultado del evento? ¿Es posible inferir de qué tipo de trampa se trata?
- ¿Algunos dominios destinatarios aparecen con mayor frecuencia en el segmento implicado, indicando un envenenamiento de las listas o la recolección de datos?
- ¿El propietario de la lista está dispuesto y puede reconstruir su lista y obtener nuevamente el permiso de los destinatarios?
- ¿Los envíos anteriores resultaron en listas de bloqueo previas? De ser así, ¿cómo se resolvió la situación?
- ¿Puede el propietario de la lista identificar la fuente de los datos problemáticos y eliminar todos los datos adquiridos a través de esa fuente?
- ¿Puede el ESP que se utilizó para enviar el mensaje obtener datos adicionales del propietario de la red de trampas de spam?

Al igual que con la verificación inicial del cliente, las áreas clave que debe analizar una auditoría incluyen la recolección, validación e higiene de las direcciones.

## Higiene de listas

Como se describe en el documento Sender Best Common Practices de M[3]AAWG (Mejores prácticas comunes para remitentes), los ESP deberían revisar el procesamiento de ciclos de retroalimentación, rebote y cancelación de suscripciones para garantizar que las direcciones de los destinatarios se procesen correctamente y se eliminen cuando sea necesario.

Los ESP también deberían revisar las prácticas de higiene de las listas de los clientes para mitigar el riesgo de enviar correo a trampas de spam. El resultado del estricto cumplimiento de las políticas detalladas en el documento de mejores prácticas para remitentes de M[3]AAWG será la reducción orgánica de los accesos a trampas de spam. Por lo tanto, se debería tener en cuenta lo siguientes:

- Si la actividad o participación de los destinatarios en un dominio en particular es menor al promedio, esto podría indicar una red de trampas de spam. Si la adquisición de direcciones en ese dominio se puede correlacionar con un segmento de lista o método de adquisición en particular, estos segmentos de lista se deberían remediar y el método de adquisición debería suspenderse.

- Los remitentes deberían considerar la implementación de una política para eliminar a los destinatarios que nunca participen o que no puedan recibir correos. Esto minimiza la posibilidad de caer en la trampa si esas direcciones se convierten en trampas recicladas. Si la incidencia de envíos a trampas continúa en su nivel actual, el remitente podría considerar la posibilidad de modificar su política existente para que sea un poco más agresiva.
- Los cambios recientes en los criterios de segmentación de listas o la gestión de archivos de supresión pueden correlacionarse con un aumento en la tasa de accesos a trampas de spam y siempre deben monitorearse de cerca. Se debe tener especial cuidado cuando el resultado de la segmentación es que reciben correo algunos destinatarios a los que no se les ha enviado por mucho tiempo, ya que durante ese tiempo una dirección puede haber sido retirada y reutilizada como trampa de spam.

En cualquier caso, un cliente o lista que produce demasiados accesos a trampas de spam debería someterse a una revisión exhaustiva. Si el cliente o la lista ya han sido sometidos a un proceso riguroso de revisión, puede que un cambio más reciente sea cómplice de una mayor actividad de trampas de spam:

- ¿Hubo algún cambio de personal en la organización del cliente?
- ¿Hay alguna nueva implementación de API o cambios recientes en una API existente que puedan haber creado oportunidades para su abuso?
- ¿Hubo cambios en los puntos de recolección de direcciones del cliente que puedan indicar un formulario web abusivo u oportunidades para envenenar la lista?
- ¿Hubo cambios organizacionales más amplios, por ejemplo, fusiones y adquisiciones o cambios en el modelo comercial, que pudieran indicar la necesidad de una nueva investigación exhaustiva del cliente?

**Eventualmente, un ESP podría encontrarse con un cliente que se niega a participar en cualquier proceso de remediación. Se recomienda enfáticamente que los ESP terminen su relación con los clientes que se nieguen a la remediación, y que consideren limitar el acceso a datos que de otro modo podrían proporcionarse a esos clientes.**

## Minimización de futuros eventos

### Prácticas de recolección de direcciones

Los ESP deberían revisar los medios que utilizan los clientes para recolectar direcciones para identificar áreas potencialmente problemáticas.

Las prácticas de recolección a veces incentivan a los consumidores a compartir una dirección de correo sin ningún tipo de verificación de los datos que garantice que la dirección pertenece a ese consumidor. Estas prácticas suelen conducir a trampas de spam en las listas. Las prácticas de recolección de mayor riesgo incluyen:

- Registros incentivados
- Registros en redes sociales
- Formularios de recomendación de amigos
- Sorteos

Las direcciones recolectadas con estas estrategias priorizan *cualquier* dirección de correo, no necesariamente la dirección *correcta*, por lo que las listas que se generan son de mala calidad.

También hay otras formas en que las trampas de spam pueden acabar en una lista, entre ellas:

- Errores tipográficos en las direcciones ingresadas en un punto de venta
- Direcciones extraídas de sitios web (ya sea de forma automática o manual)
- Listas compradas, alquiladas o *e-pended*
- Listas de participantes en ferias comerciales.
- Formularios de registro de adhesión (*opt-in*)

Al investigar las prácticas de recolección de direcciones, los ESP deben solicitar los datos de adhesión específicos del cliente. Una técnica de investigación común consiste en proporcionar múltiples direcciones al cliente, entre ellas algunas direcciones que no están en la lista. Luego, se solicita al cliente que proporcione los datos de adhesión, entre ellos:

- La fecha y hora de registro
- La URL del formulario utilizado y la IP de conexión (si el registro se realizó en línea)
- El lugar donde se realizó la transacción, si la dirección se obtuvo en persona.

Los clientes deberían poder proporcionar datos específicos de la adhesión, incluidos, entre otros, la URL de cualquier formulario web. Como a veces se agregan trampas de spam a las listas mediante el envío de formularios automatizados, los clientes y los ESP deberían revisar los análisis de tráfico del sitio web. Un tráfico no tradicional o picos inusuales en el volumen podrían indicar que un formulario se ha convertido en el blanco de bots, lo que genera un aumento de las trampas de spam en una lista.

Los ESP también pueden verificar si los procesos de adhesión funcionan de la forma prevista. ¿El resultado de un registro en la URL proporcionada por el propietario de la lista en el momento de la auditoría es una suscripción verificable? De no ser así, considere la posibilidad de que las URL proporcionadas no pertenezcan al propietario de la lista o que los registros desde la página se compartan entre muchos. Verifique si existe algún mecanismo de confirmación y si funciona según lo previsto.

## Validación en el punto de recolección

Los clientes pueden complementar las buenas prácticas de recolección incorporando estrategias de validación de direcciones de correo electrónico. Esta validación puede ser mediante una revisión interna en el ESP, o usando uno de los numerosos servicios que ofrecen validación a demanda o en el momento de la recolección de la dirección. La mejor práctica consiste en validar la dirección cuando el suscriptor la ingresa y solicitarle que vuelva a ingresarla si la validación falla.

Si la validación se realiza internamente, hay una serie de pistas que los ESP pueden buscar en una lista y que podrían indicar estrategias de validación deficientes o inexistentes. M$^3$AAWG Vetting Best Common Practices ofrece una descripción completa de estas estrategias.

## Otras estrategias de prevención

También hay otras acciones que se pueden considerar para reducir problemas futuros. Estas incluyen limitar la capacidad del cliente para importar listas, por ejemplo, al permitir que las direcciones se agreguen exclusivamente mediante un script de formulario proporcionado por el ESP o mediante algún otro proceso.

También se pueden aplicar restricciones al envío, como enviar únicamente a segmentos comprometidos o

exigir al remitente que, como paso adicional, elimine o suprima los segmentos que muestren poca o ninguna interacción histórica. Por sobre todo, se debe exigir al cliente que descarte los segmentos que no tengan permisos confirmados, aunque se podría permitir que el cliente primero intente reconfirmar sus permisos.

Si un cliente es parte de un entorno compartido, podría ser necesario aislar a ese cliente en una infraestructura dedicada para minimizar el potencial daño a la reputación de otros remitentes que utilicen la misma infraestructura compartida.

## Conclusiones

Cuando nuestro sistema cae en una trampa de spam, hay muchas cosas que se deben considerar. Los ESP deben proteger su infraestructura, pero también deben evaluar a los clientes que caen en esas trampas. En definitiva, la trampa de spam no es el problema, sino una señal de un problema subyacente que tiene que ver con cómo el cliente adquiere y valida las direcciones. Las trampas de spam son una forma de identificar técnicas deficientes para la recolección de direcciones. Las trampas en sí son un indicador de que en la lista hay direcciones que carecen de permiso. En muchos casos, estas direcciones pertenecen a personas reales que están recibiendo spam. Al arreglar los procesos de recolección que conducen a trampas de spam, también se está abordando el spam que está afectando a personas reales. La principal preocupación siempre deben ser los destinatarios que puedan estar recibiendo spam. Existen muchas estrategias efectivas; este documento ofrece un punto de partida para abordar el problema.

## Referencia


- En el sitio web de M³AAWG's, ver "Documents for Senders and ESPs"
  https://www.m3aawg.org/documents-for-senders-and-esps
  y en particular
- M³AAWG Sender Best Common Practices, versión 3.0, actualizado en febrero de 2015
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- M³AAWG Best Current Practices for Building and Operating a Spam Trap, versión 1.2.0, actualizado en agosto de 2016
  https://www.m3aawg.org/documents/en/m3aawg-best-current-practices-for-building-and-operatin g-a-spamtrap-ver-120
- Vetting Best Common Practices (BCP), noviembre de 2011
  https://www.m3aawg.org/sites/default/files/document/MAAWG_Vetting_BCP_2011-11.pdf


Al igual que para todos los documentos que publicamos, consulte el sitio web de M³AAWG (www.m3aawg.org) para ver las últimas actualizaciones.