SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
Servicio de Administración Tributaria

Recomendaciones y acciones solicitadas al contribuyente

que ha recibido un correo apócrifo del SAT

¿QUÉ ES UN CORREO ELECTRÓNICO APÓCRIFO?

Es un correo electrónico que a través de suplantación de identidad intentan obtener información personal o confidencial de la víctima, por ejemplo usuarios y contraseñas.

El Servicio de Administración Tributaria ha identificado el envío de correos electrónicos que no pertenecen a la entidad y que buscan engañar a los contribuyentes para conseguir sus datos personales. Dichos mensajes pretenden sorprender a los ciudadanos ya que advierten sobre supuestas irregularidades fiscales o citas, donde solicitan llenar formularios con datos generales, e incluso de alguna tarjeta de crédito para devolverle un aparente saldo a favor o evitar supuestas acciones legales, o actualizar sus datos. En algunos casos se pide seguir un enlace o descargar archivos que contienen algún malware (virus informático).

A continuación se muestra un ejemplo de correo electrónico apócrifo:

¿Cómo puedo identificar un correo apócrifo?

- Revisa la cuenta origen del correo electrónico, esta puede ser parecida a la de empresas e instituciones reconocidas, pero levemente alterada. Ejemplo:
    - Notificacion SAT @mobil..com
    - SAT@hotmail.com
    - SAT <evengage@asia.com>
    - Avisos SAT <administración@serviciosat.net>
- Puedes comparar la cuenta que envía el correo electrónico con la lista de cuentas identificadas por el SAT dentro del siguiente portal:
    - https://www.gob.mx/sat/acciones-y-programas/lista-de-correos-apocrifos-identificados?state=published
- Si tu cuenta de correo electrónico no se encuentra dentro de los destinatarios, revisa con mayor cuidado.
- Los correos electrónicos apócrifos contienen (cuentan con errores de gramática o de ortografía.
- Revisa el contenido del correo electrónico, ya que puede contener enlaces a sitios web no confiables que solicitan información personal, o descarga de archivos.
- Una manera de identificar si los sitios contenidos en el cuerpo del correo electrónico son maliciosos es colocando el puntero del mouse en el vínculo y observar la dirección que aparece en el recuadro, la cual podría ser diferente a la que aparece en el cuerpo del correo

Ejemplo:

- El SAT no distribuye software, no solicita ejecutar o guardar un archivo ni requiere información personal, claves o contraseñas por correo electrónico. Si recibes algún mensaje de este tipo repórtalo a través de Quejas en los servicios por internet o en el correo denuncias@sat.gob.mx, siguiendo las instrucciones del apartado "REPORTAR UN DE CORREO ELECTRÓNICO APÓCRIFO"

Recibí un correo electrónico apócrifo ¿Cómo me protejo?

- No accedas a sitios web de dudosa reputación.
- NO ejecutes archivos sospechosos que se encuentren adjuntos al correo electrónico o se descarguen de enlaces sospechosos.
- Evitar el ingreso de información personal en formularios de sitios sospechosos.
- Utilizar contraseñas fuertes y realizar un cambio programado de las mismas.
- Mantén actualizado tu sistema anti-virus.
- Reporta el correo sospechoso a través del área de Quejas en los servicios por internet o en el correo denuncias@sat.gob.mx.

COMO REPORTAR UN CORREO ELECTRÓNICO APÓCRIFO

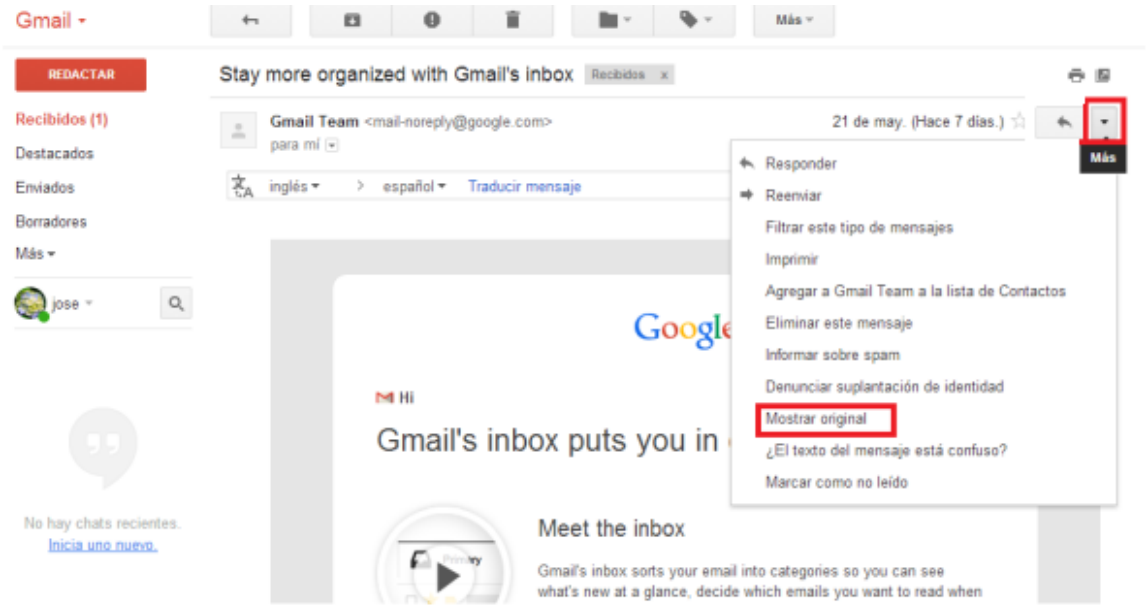
Para reportar un correo electrónico apócrifo reenvía el correo recibido y el código fuente del correo apócrifo adjuntos a la cuenta de denuncias@sat.gob.mx; para ello realiza las siguientes acciones:

Paso 1

Obtén el código fuente del correo. Si tienes cuenta en Hotmail, Yahoo!! o Gmail realiza lo siguiente:

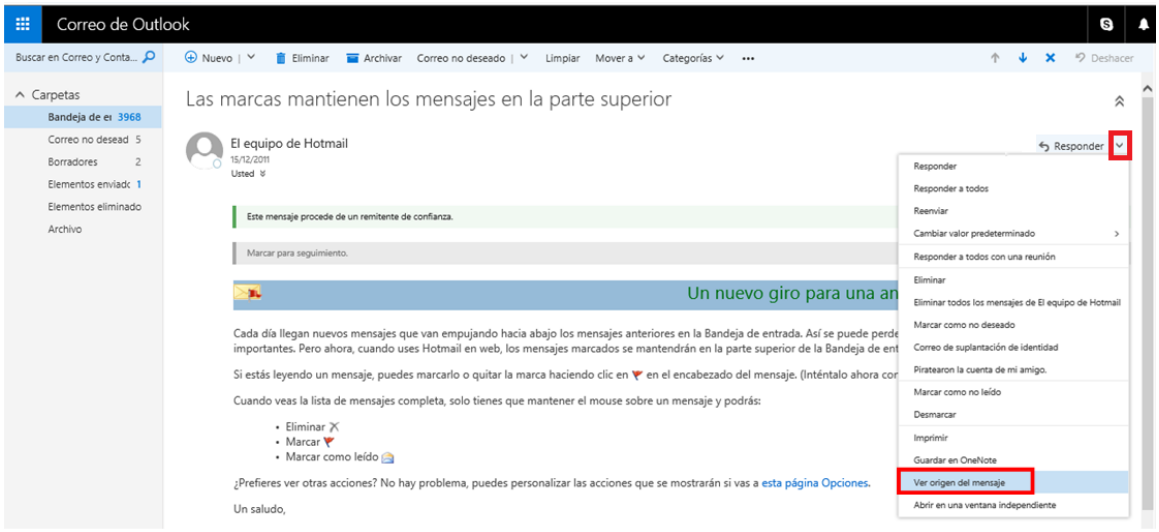
Gmail

Accede al correo electrónico sospechoso y de clic en la flecha que se encuentra a lado del campo responder, como se muestra en la imagen siguiente, se desplegará una lista de opciones, seleccione “Mostrar original”



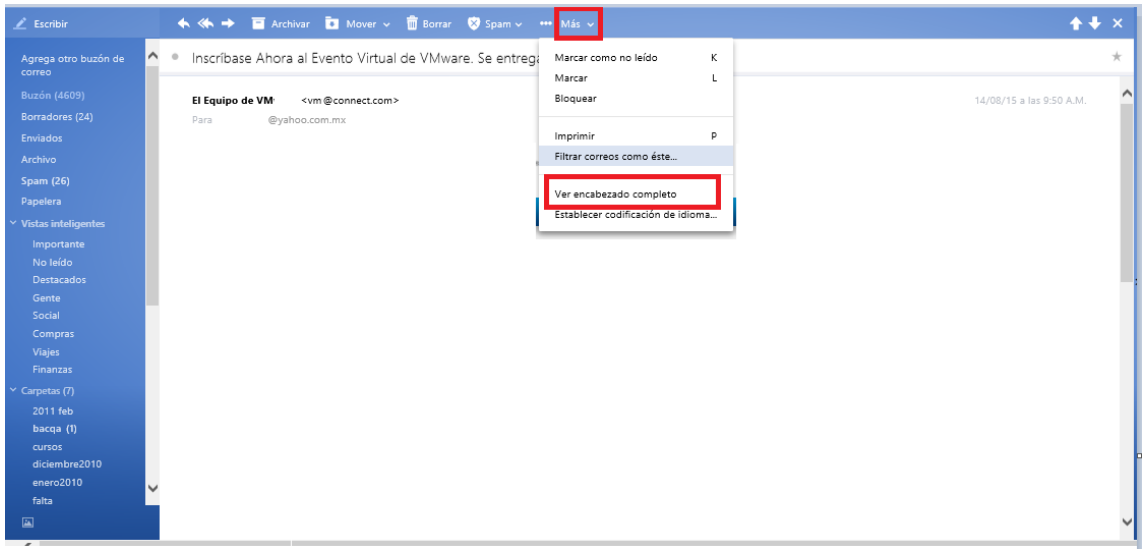
Hotmail, Outlook

Accede al correo electrónico sospechoso y da clic en la flecha que se encuentra a lado del campo “Responder” como se muestra en la imagen siguiente, se desplegará una lista de opciones, seleccione “Ver origen del mensaje”



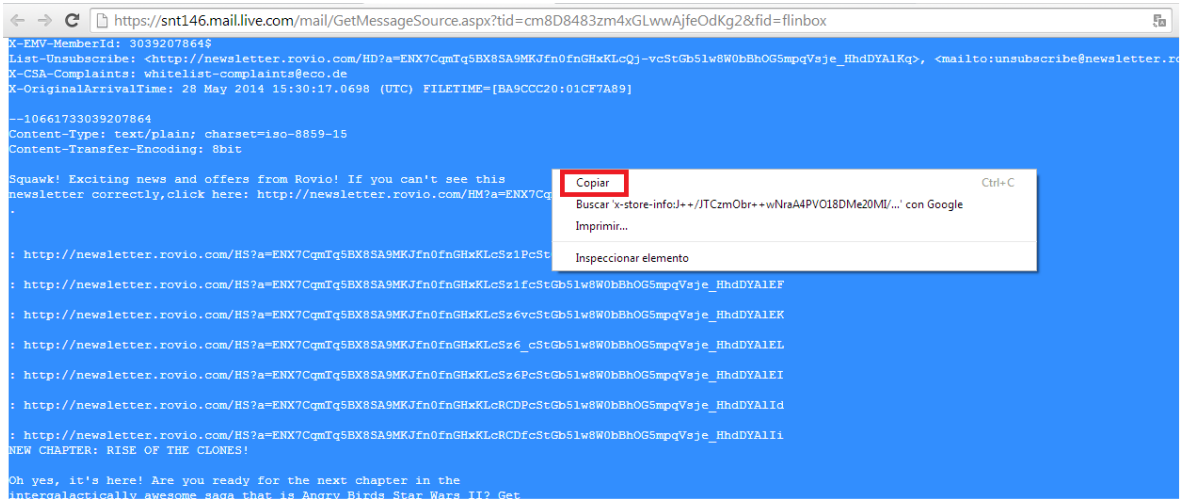
Yahoo!

Accede al correo electrónico sospechoso y da clic en la flecha que se encuentra a lado del campo “Más” como se muestra en la imagen siguiente, se desplegará una lista de opciones, seleccione “Ver encabezado completo”



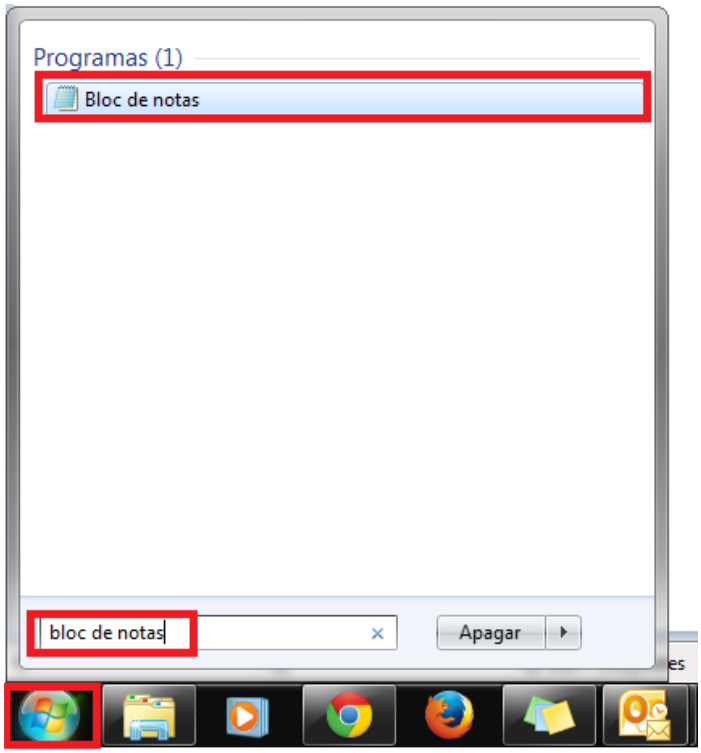
Paso 2

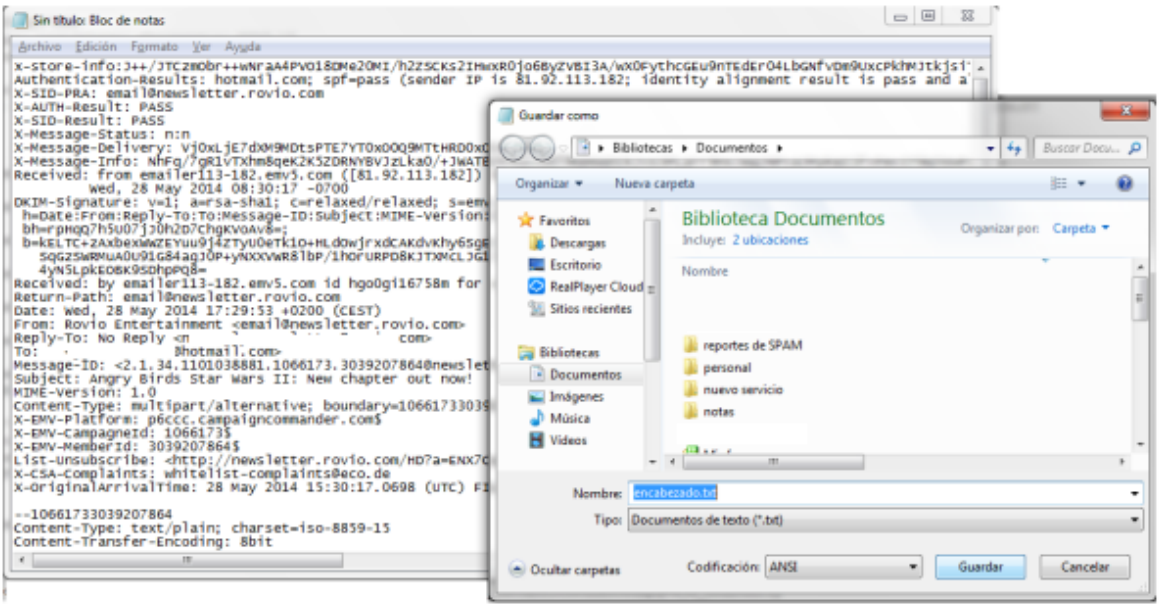
Selecciona el texto que se muestra en la nueva pantalla y copia la información.



Paso 3

Pega la información en un archivo de texto y envíalo adjunto a denuncias@sat.gob.mx.





Recomendaciones en materia de seguridad

- Utiliza claves fáciles de recordar, pero difíciles de adivinar con un mínimo de ocho caracteres, donde existan al menos una letra en mayúsculas y alguno de los símbolos: &, %, $, @, etcétera.
- Cambia las contraseñas de manera regular.
- Procura utilizar contraseñas diferentes si tienes servicios por internet en más de un banco.
- Desactiva la opción Recordar contraseñas en el explorador de internet.
- Mantén instalado y actualizado un sistema antivirus.
- No descargues o abras archivos que se encuentren dentro de correos electrónicos sospechosos.
- En caso de haber descargado o ejecutado algún archivo dentro de las ligas maliciosas contenidas en el correo electrónico apócrifo, realiza un escaneo manual del equipo con tu sistema antivirus actualizado.