



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

LA IMPORTANCIA DE LOS ARCHIVOS EML Y CABECERA



PROCEDIMIENTO PARA
ADJUNTAR UN ARCHIVO EML
Y CABECERA EN OUTLOOK





El correo electrónico es uno de los principales medios utilizados por los ciberdelincuentes para cometer estafas, como el phishing. Para comprobar si un mail es malicioso y analizar su contenido, es necesario tener el detalle completo del correo, el que se conserva en su archivo **EML y en la cabecera**. Si quieres reportar un phishing con la información completa, adjuntar estos elementos resulta esencial. A continuación te explicamos paso a paso cómo hacerlo.



PRECAUCIONES ANTES DE INICIAR ESTE PROCEDIMIENTO

Antes de realizar este procedimiento, toma las siguientes precauciones:

-  Nunca abras el archivo que viene adjunto en un phishing.
-  No ingreses a los enlaces que vienen en el correo.
-  No entregues ningún tipo de datos, menos aún personales o confidenciales.
-  No respondas los phishing, ni por curiosidad.

¿QUÉ ES UN ARCHIVO EML?

Es un correo electrónico archivado que preserva el formato y las cabeceras HTML originales. Este archivo se puede obtener desde todos los servicios de correo electrónico.

¿QUÉ ES UNA CABECERA?

Un correo tiene dos partes: la cabecera y el contenido del mensaje. De la cabecera se puede obtener el remitente real y el remitente suplantado, además de información como el destinatario, la fecha, los servidores implicados en la transmisión del remitente al destinatario, entre otros. Por eso, es importante contar con esta información para analizar un phishing.

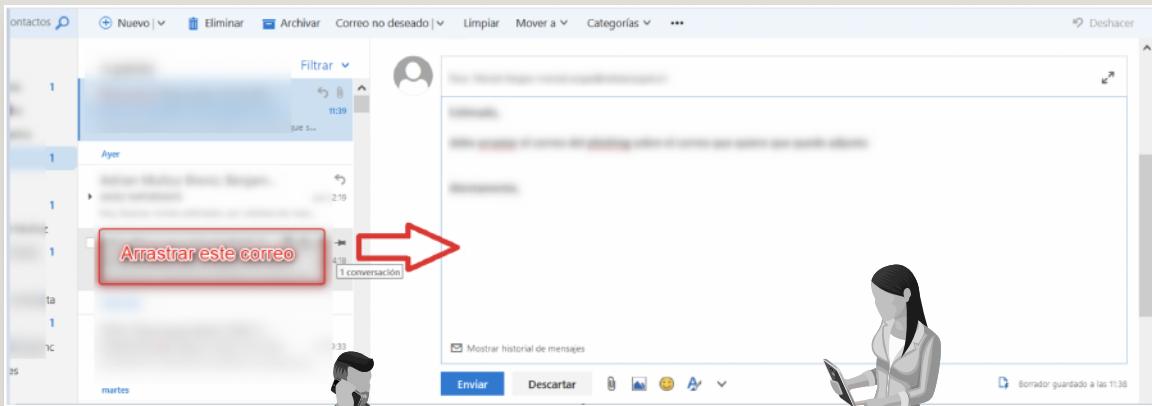


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo
EML / OUTLOOK WEB

1.

Primero, debes crear un nuevo correo. Luego, "toma" el correo del phishing y arrástralo sobre el nuevo correo en el cual lo quieras "adjuntar" y guárdalo hasta que obtengas la cabecera.



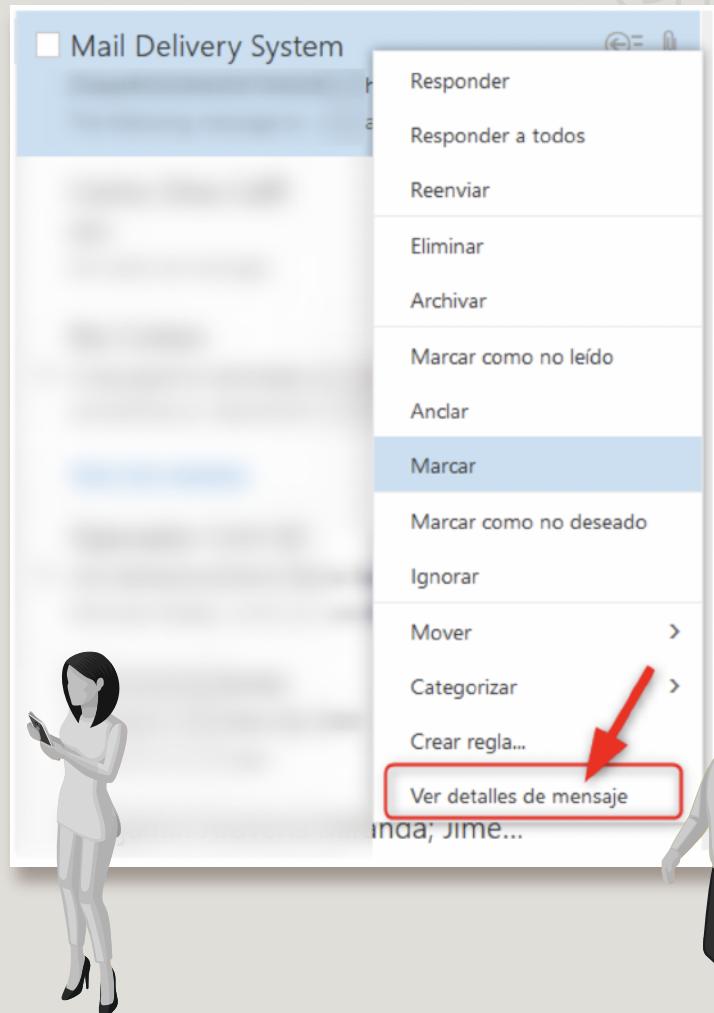


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo **CABECERA/ OUTLOOK WEB**

1.

Haz clic con el botón derecho sobre el phishing recibido y selecciona "Ver detalles del mensaje"



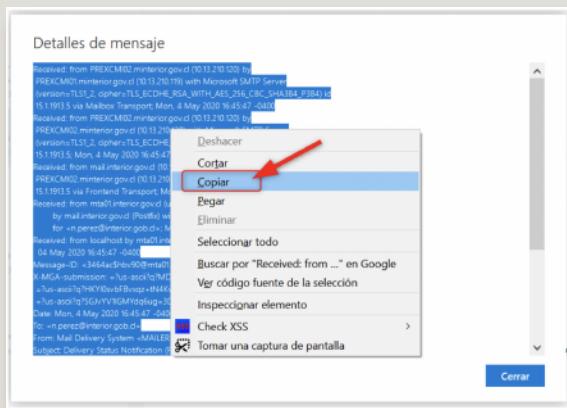


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo CABECERA/ OUTLOOK WEB

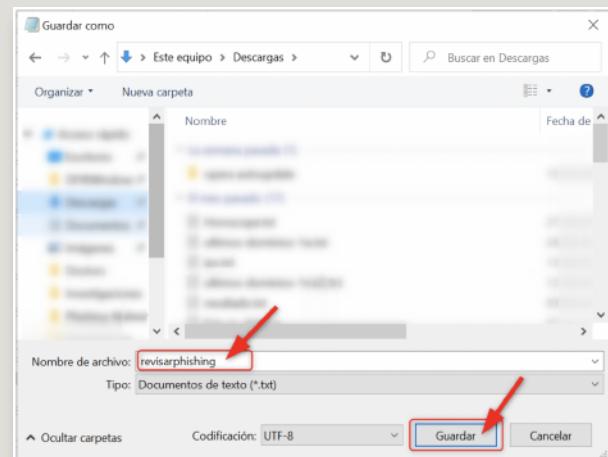
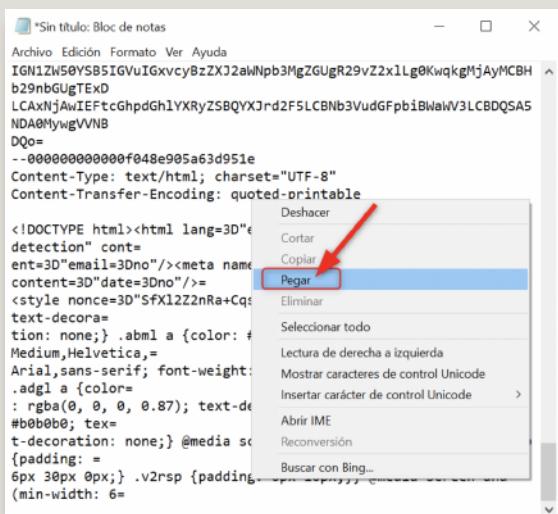
2.

Selecciona todo el texto que aparecerá en “Detalles de mensaje”, copia todo el texto y pégalo en un block de notas.



3.

Guarda el bloc de notas con el nombre que prefieras.
De esta manera obtienes la cabecera del correo del
phishing que se debe enviar para análisis.



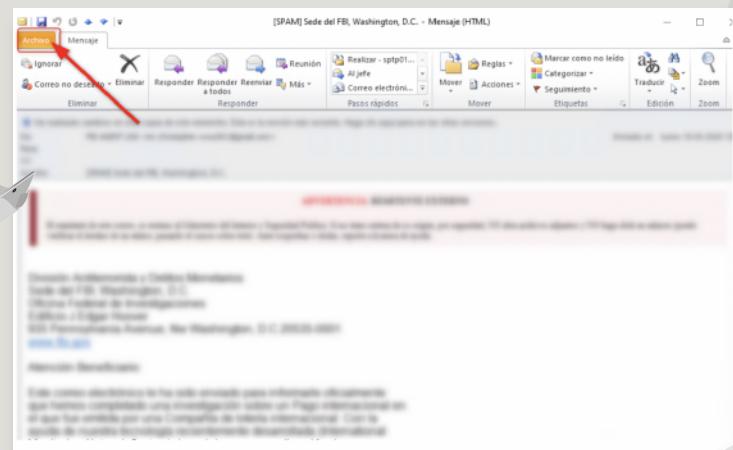


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo EML/ OUTLOOK APLICACIÓN

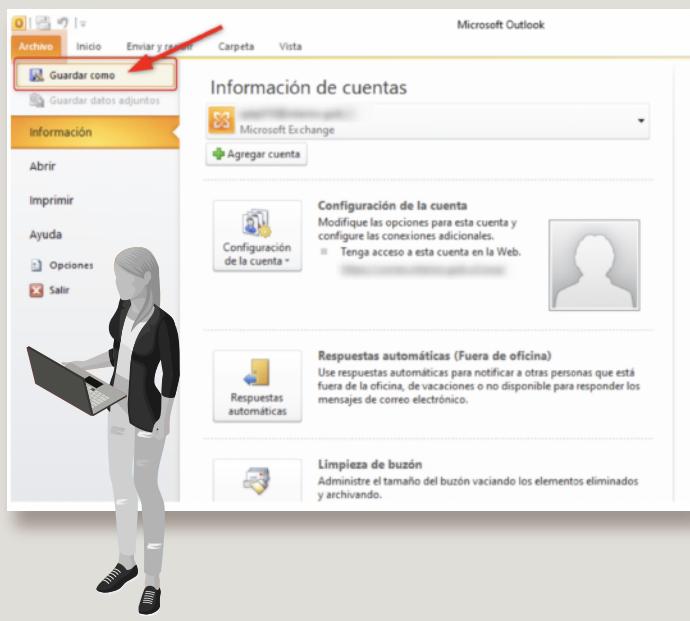
1.

Abre el correo que quieras enviar y selecciona la opción "Archivo" que está arriba a la izquierda.



2.

Abre el correo que quieras enviar y selecciona la opción "Archivo" que está arriba a la izquierda.



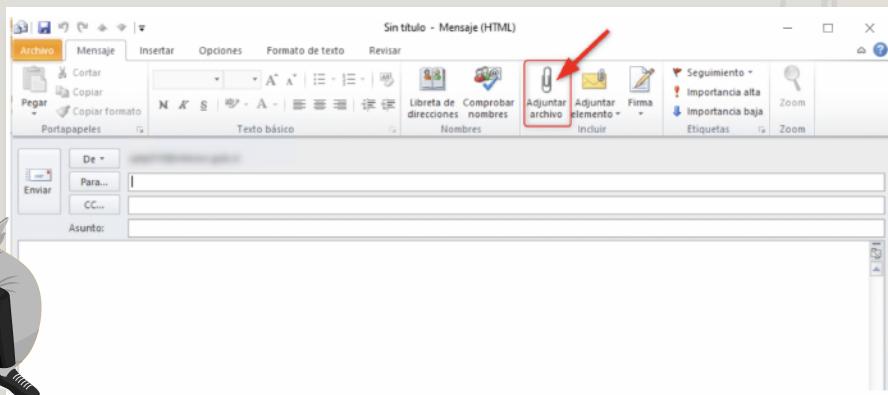


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo EML/ OUTLOOK APLICACIÓN

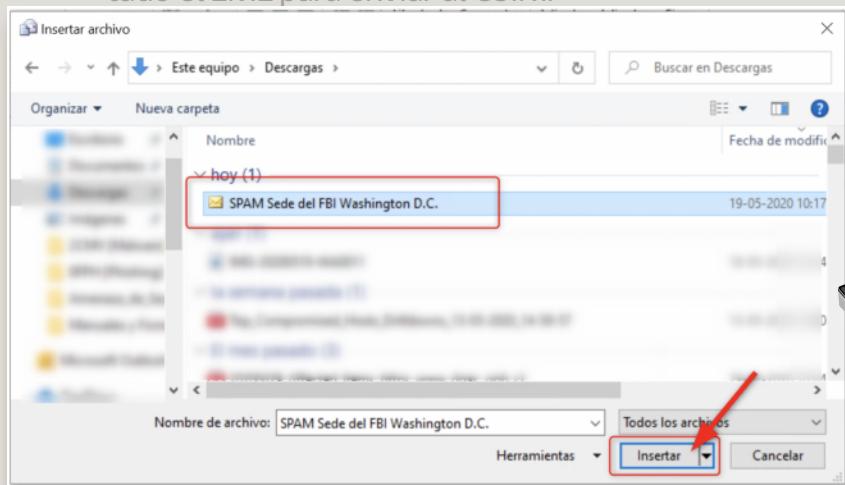
3.

Posteriormente, crea un nuevo correo electrónico y “adjunta” el correo que acabas de guardar (EML).



4.

Selecciona el correo recién guardado y dirígete a “Insertar”, así estarás adjuntando el EML para enviar al CSIRT.



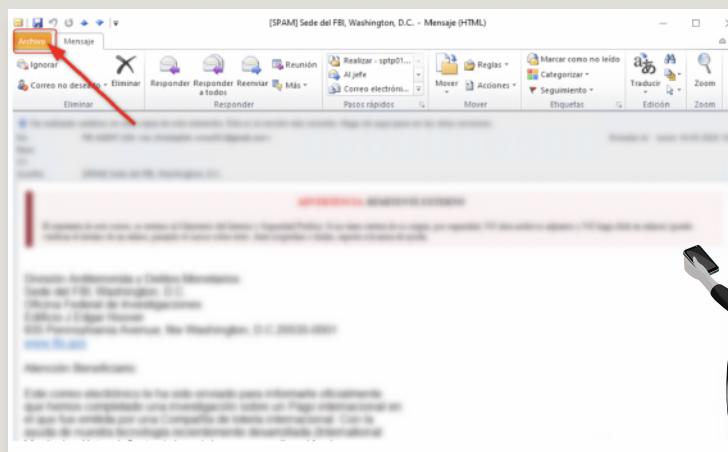


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo **CABECERA/ OUTLOOK APLICACIÓN**

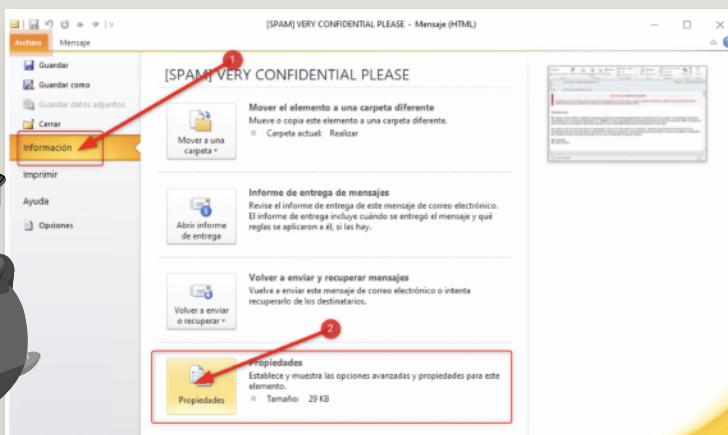
1.

Dirígete a la esquina superior izquierda
y selecciona "Archivo".



2.

Se desplegará un menú al lado
izquierdo, selecciona "Información"
y luego "Propiedades".



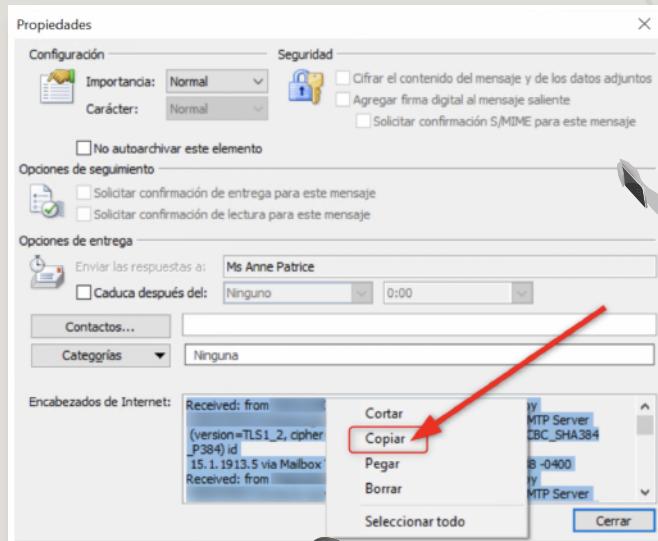


PROCEDIMIENTO PARA ADJUNTAR UN ARCHIVO EML Y CABECERA EN OUTLOOK

archivo **CABECERA/ OUTLOOK APLICACIÓN**

3.

Aparecerán diversas opciones. Dirígete al final a la sección “Encabezados de Internet”, selecciona todo el texto, cópialo, pégalo en un bloc de notas y lo adjuntas en el correo para analizar.





Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl