CIBERCONSEJOS

SPOOFING DE EMAIL

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

¿Qué es el spoofing?

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Es una de las técnicas usadas por los ciberdelincuentes para engañar a las personas y suplantar de forma más convincente la identidad de una persona, empresa o fuente confiable. Esto, con el objetivo de obtener información confidencial, acceder a sistemas o redes, o realizar acciones fraudulentas.

Las técnicas del spoofing de email, por ejemplo, se implementan para aumentar las probabilidades de éxito de un ataque de phishing.

Existen varios tipos de spoofing, incluyendo el de correo electrónico, IP y DNS, entre otros. El más relevante para los usuarios finales es el spoofing de email.

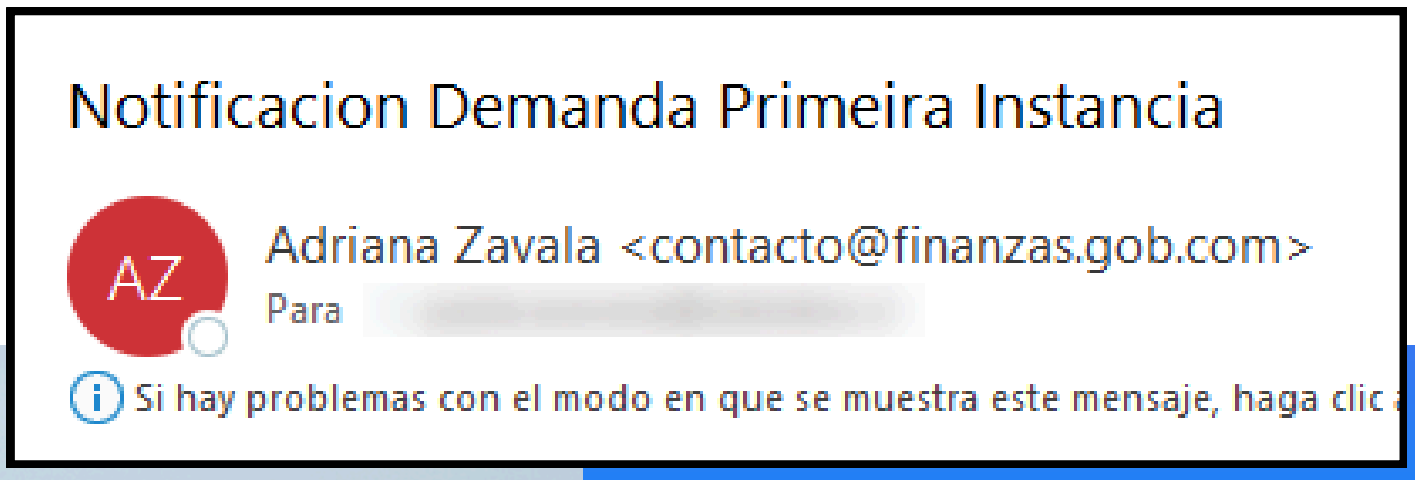
Spoofing de correo electrónico

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

El atacante genera un encabezado de email engañoso, ya sea usando técnicas para mostrar una dirección de correo que realmente emplea la persona que está siendo suplantada, o creando direcciones falsas, pero que en una mirada rápida parecen ser legítimas.

Lo primero es posible porque la infraestructura de correos electrónicos usada por la entidad suplantada está mal configurada, ya que no limita el envío de mensajes en su dominio solo a sus usuarios autentificados ni solo desde sus servidores de correo.

Abajo vemos un ejemplo de un email que muestra un remitente falso pero que podría parecer creíble:



No caigas con el spoofing de emails

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- Fíjate en que el remitente del email sea el que realmente debería ser. Atento a direcciones parecidas a las legítimas, pero que no lo sean, como en el ejemplo anterior.

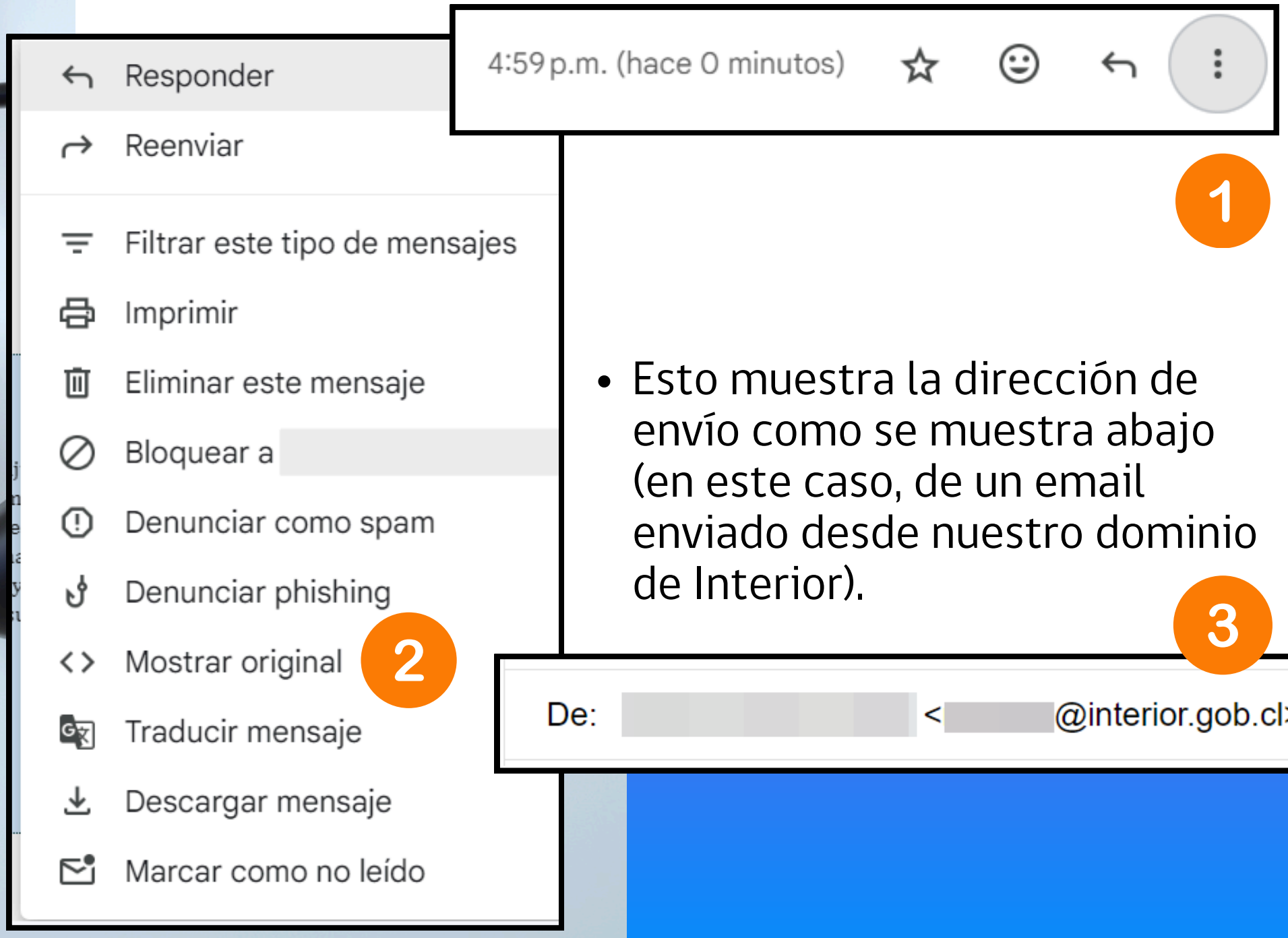
- Usa direcciones de correo “desechables” para registrarte en sitios que no sean importantes para ti. Así, de caer esa dirección en malas manos y la usan para enviarte phishing con spoofing, será menos probable que caigas.

- Utiliza servicios de email que cuenten con protocolos más seguros que reducen la efectividad del spoofing, como DMARC, DKIM y SPF, además de filtros de spam. Consulta a los responsables de tecnología de tu institución para saber si tu correo laboral cuenta con esta tecnología.

No caigas con el spoofing de emails

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

- Revisa que la dirección mostrada en el encabezado sea la misma usada para entregar el email. En Gmail (de escritorio) puedes seleccionar “Mostrar original” en el menú de los tres puntitos.



- Esto muestra la dirección de envío como se muestra abajo (en este caso, de un email enviado desde nuestro dominio de Interior).

Otros tipos de spoofing

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Spoofing de IP

Suplantación de una dirección IP, que busca engañar principalmente a redes computacionales y así lograr entrar a estas sin autorización.

Spoofing de DNS

El objetivo del sistema DNS es asignar nombres fáciles de usar a una dirección IP. Con la suplantación de DNS, el atacante altera la información del servidor DNS para redirigir a las víctimas a sitios web fraudulentos, haciéndoles creer que están accediendo a sitios legítimos.