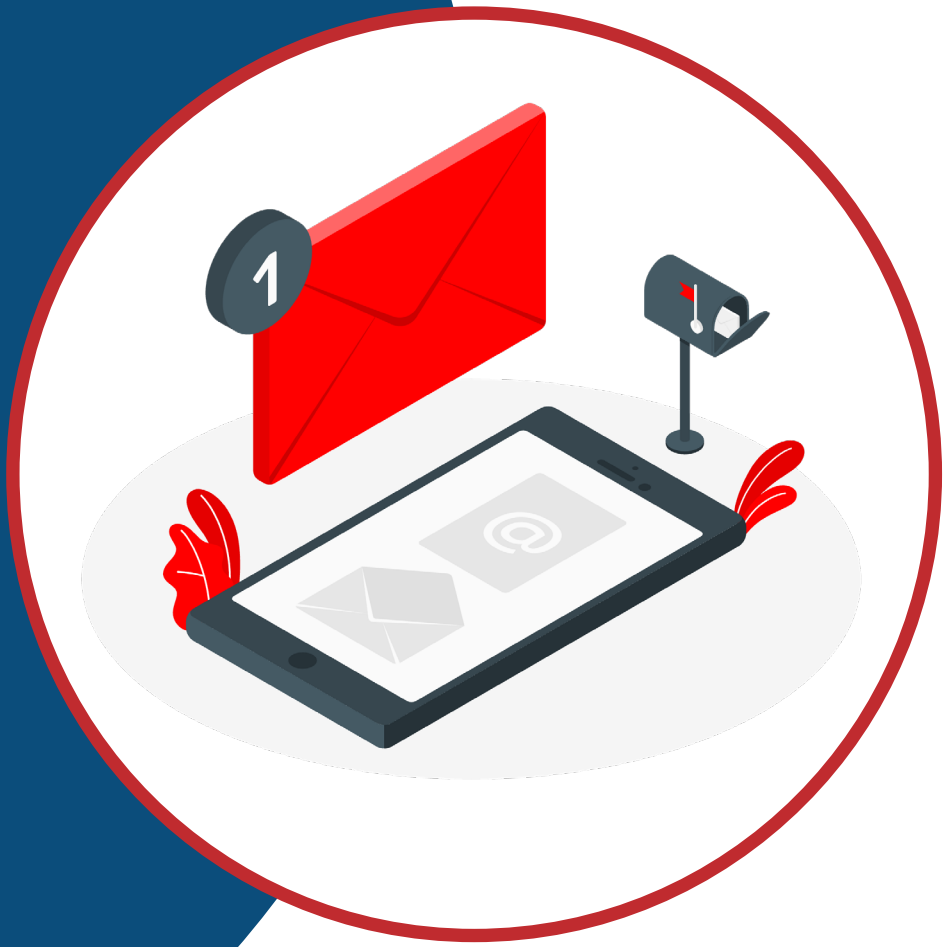
CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERGUÍA
EMAIL SPOOFING

SUPLANTACIÓN DE IDENTIDAD VÍA CORREO



https://www.csirt.gob.cl/

¿QUÉ ES EL SPOOFING?

Es una técnica utilizada por los ciberdelincuentes para engañar a las personas, suplantando la identidad de una persona, empresa o fuente confiable, con el objetivo de obtener información confidencial, acceder a sistemas o redes, o realizar acciones fraudulentas. Existen diferentes tipos de spoofing, incluyendo el de correo electrónico, IP y DNS, entre otros.

EMAIL SPOOFING

Es la forma más utilizada de suplantación de identidad, en donde el ciberdelincuente envía correos haciéndose pasar por una persona o empresa para que proporcione información sensible, descargue un malware o para extorsionar exigiendo un pago en criptomoneda.

En estos casos, se genera un encabezado o remitente del email engañoso, ya sea mostrando la misma dirección de correo de la persona que está siendo suplantada, o creando direcciones falsas, pero que en una mirada rápida parecen ser las reales.

EJEMPLO I
EMAIL SPOOFING

De: [redacted]
Fecha: [redacted]
Para: [redacted]
Asunto: A la espera del pago.

¡Hola!
¿Ha notado hace poco que ha recibido un correo electrónico desde su propia cuenta?
Eso es simplemente porque tengo total acceso a su dispositivo.

Llevo un par de meses observándole.
¿No entiende cómo es posible? Bueno, ha sido infectado con un malware originario de un sitio web para adultos que visitó. Por si no está familiarizado con estos temas, intentaré explicárselo.

Con la ayuda de un virus troyano, puedo obtener total acceso a un PC o a cualquier otro dispositivo.
Eso significa que puedo verle siempre que quiera frente a la pantalla, con solo encender la cámara y el micrófono sin que usted se dé cuenta.
Además, también tengo acceso a su lista de contactos y a todos sus mensajes de correo.

Puede que se pregunte: "Pero mi PC tiene un antivirus activo, ¿cómo es posible? ¿Por qué no he recibido ninguna notificación?"
La respuesta es sencilla: mi malware utiliza controladores, lo que me permite actualizar las firmas cada cuatro horas y hacer que sea indetectable, y por eso el antivirus se mantiene en silencio.

Tengo un vídeo en el que sale masturbándose en el lado izquierdo, y en el derecho la película que estaba viendo mientras se masturbaba.
¿Se está preguntando en qué puede perjudicarle esto? Con un solo clic de ratón, puedo enviar el vídeo a todas sus redes sociales y contactos de correo electrónico.
También puedo compartir todos sus mensajes de correo electrónico y de messenger.

Lo único que debe hacer para evitar que esto suceda es transferir bitcoins por valor de 750$ USD a mi dirección bitcoin (si no tiene ni idea de cómo hacerlo, puede abrir el navegador y simplemente buscar: "Comprar bitcoins").

Mi dirección bitcoin (monedero de bitcoin) es: [redacted]

Una vez que reciba la confirmación del pago, borraré el vídeo de inmediato, y se acabó, no volverá a saber de mí.
Tiene 2 días (48 horas) para completar esta transacción.
Cuando abra este mensaje de correo, recibiré una notificación y mi temporizador se pondrá en marcha.

Presentar una denuncia no le servirá de nada, ya que este correo electrónico no puede ser rastreado, al igual que mi identificador bitcoin.
Llevo mucho tiempo dedicándome a esto y nunca cometo errores.

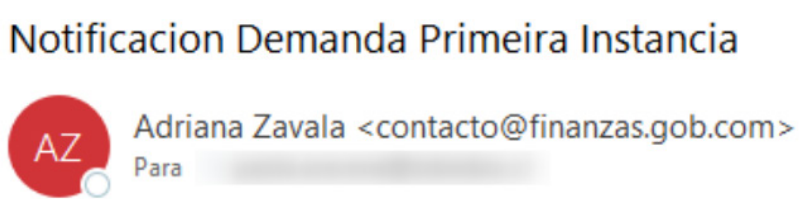
Si descubro que ha compartido este mensaje con alguien más, distribuiré inmediatamente el vídeo, tal como le he advertido.

CORREO CON MISMO NOMBRE DE EMAIL

En el ejemplo, el ciberdelincuente envía un correo aparentando ser desde la misma cuenta de la persona suplantada, señalando que tiene control total no solo de la cuenta de correo, sino que también del dispositivo donde se utiliza, para extorsionar con la publicación de un supuesto vídeo íntimo, si no se realiza un pago en criptomoneda.

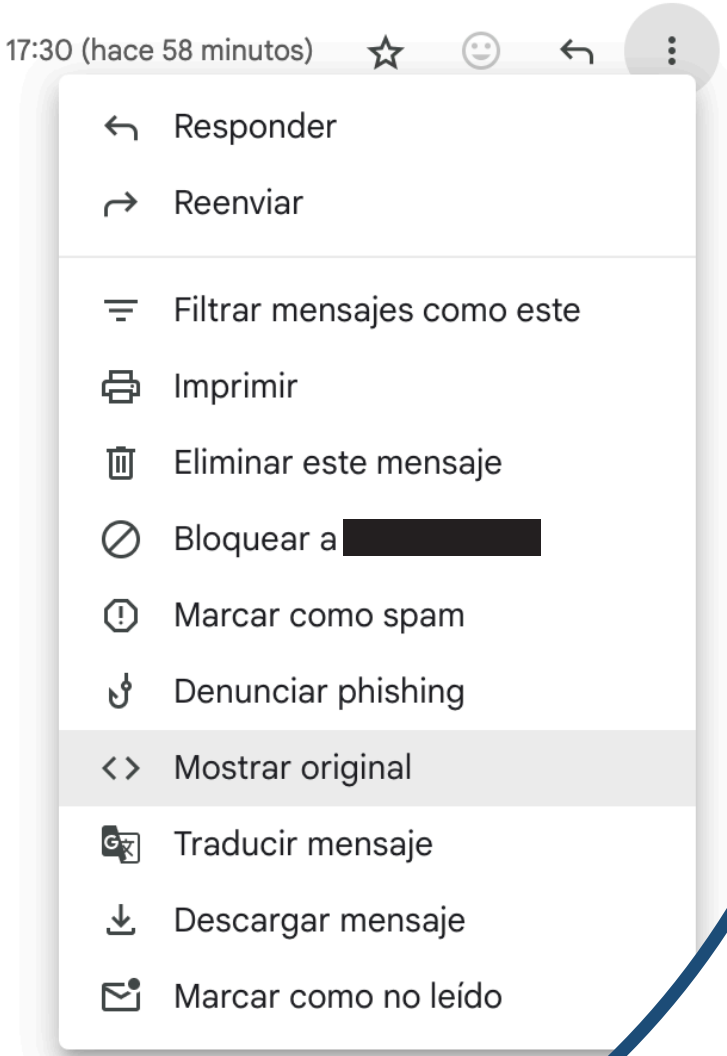
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

EJEMPLO II
EMAIL SPOOFING



CORREO CON NOMBRE QUE SIMULA SER OFICIAL

En este caso el ciberdelincuente envía un correo con remitente falso, pero que a primera vista, podría ser creíble como real.



¿CÓMO EVITAR SER VÍCTIMA DEL EMAIL SPOOFING?

- **Asegúrate de que el remitente del correo electrónico sea auténtico. Presta atención a direcciones que parecen legítimas pero que contienen pequeñas diferencias.**
- **Desconfía de correos extorsivos que te solicitan dinero de manera urgente.**
- **Para registrarte en sitios que no consideres importantes, emplea direcciones de correo temporales. De esta manera, si esa dirección es comprometida y utilizada para enviarte phishing mediante spoofing, será menos probable que te engañen.**
- **Opta por servicios de correo electrónico que implementen protocolos avanzados de seguridad, como DMARC y SKIP, junto con filtros de spam. Consulta con el equipo de tecnología de tu organización para verificar si tu correo laboral está protegido con estas tecnologías.**
- **Verifica que la dirección mostrada en el encabezado del correo coincida con la dirección utilizada para enviar el mensaje. En Gmail (versión de escritorio), puedes seleccionar “Mostrar original” en el menú de los tres puntos para ver la dirección de envío real.**

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

https://www.csirt.gob.cl/

Síguenos en nuestras redes sociales:

Teatinos 92 piso 6. Santiago, Chile

Abril 2024