

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	8FPH23-00907-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de noviembre de 2023
Última revisión	13 de noviembre de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER [ACÁ](#)

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente:

“Un nuevo navegador web ha iniciado sesión en su cuenta de Webmail. Para ayudar a mantener su cuenta segura, háganos saber si este es usted.”

El correo electrónico incluye un enlace a un formulario para capturar credenciales de usuarios.

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Indicadores de compromiso

Antes de evaluar la aplicación de acciones, tenga presente las advertencias de **gestión de los IoC**. Los IoC de este informe pueden ser obtenidos directamente desde nuestro **repositorio**.

URL del sitio falso

https://pub-2e883b09c0a74dc48174fe1ca14292cf.r2[.]dev/mailbox-protection.html

URL de redirección

N/A

IP del sitio falso

104.18.2.35

Asuntos del correo electrónico

we noticed a new sign in to your webmail account
--

Correos de salida

noreply@bst.ppmhospital.com

IP	Comentario
185.236.231.195	SMTP

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Imágenes Relacionadas

Hi soc-csirt, we noticed a new sign in to your webmail account soc-csirt@interior.gob.cl

ST Support Team <[redacted]>
Para [redacted] lu. 13/11/2023 1:24

Responder Responder a todos Reenviar

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Pública. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.

Hi [redacted]

A new web browser signed in to your Webmail account. To help keep your account secure, let us know if this is you.

Is this you?

When: Nov 10, 2023 at 12:35 pm (WAT)
What: Chrome on Windows

Yes No

[I'm not sure](#)

Learn more on how to [protect your account](#).

Thanks,
- The Webmail Team



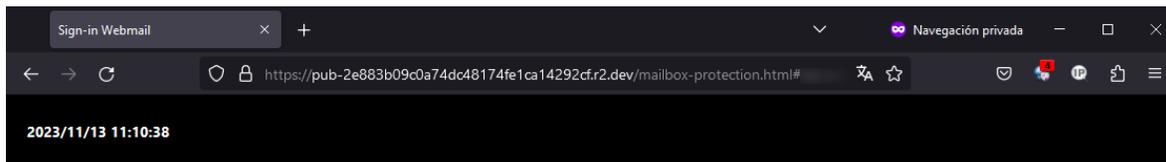
Imagen 1: Correo Electrónico

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Email Settings | For: INTERIOR
Secured 2023. All rights reserved.

Imagen 2: Sitio fraudulento

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>