

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior

| | |
|---------------------------------|--------------------|
| Alerta de seguridad informática | 8FPH23-00827-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 31 de mayo de 2023 |
| Última revisión | 31 de mayo 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:

“Le informamos que el proceso de actualización de datos esta a punto de expirar, si no realiza hoy se procederá con el bloqueo de su cuenta.”

De abrir el enlace, la persona es dirigida a un sitio falso semejante a los de Banco Ripley, donde se expone al robo de su usuario y contraseña (credenciales).

IoC Correo Electrónico

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](#). De forma preventiva, sugerimos aplicar las siguientes [recomendaciones](#) de ciberseguridad.

URL redirección:

<https://bit.ly/3oMxl6V?l=www.bancoripley.cl>

URL sitio falso:

<https://web.bancoripley-cl.grfer.com.br/1685557879/login/index.html>

Dirección IP del sitio falso:

[108.167.171.58]

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@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
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior




Datos del remitente:

| Asunto | Correo de Salida | SMTP Host |
|--|--------------------------------|------------------|
| Fwd_ Actualiza tus datos hoy y Gana ,mas info aqui | ortozone@node3325.myfcloud.com | [172.104.132.96] |


Imagen del mensaje

Fwd: Actualiza tus datos hoy y Gana € ,mas info aqui³.

 BancoRipley <noreply@publmail.com>
Para



   Responder  Responder a todos  Reenviar 

mi. 31/05/2023 13:01

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



CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@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
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior

Imagen del sitio



CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

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