

## Alerta de Seguridad Informática (8FPH-00032-001)

**Nivel de Riesgo: Alto**

**Tipo: Phishing**

Fecha de lanzamiento original: 20 de Junio de 2019 | Última revisión 20 de Junio de 2019

### Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

---

### Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Scotiabank. El correo trata de persuadir al cliente que tiene que aprobar un abono, ya que fue premiado por un aumento de su línea de crédito de \$ 999.999 y además participara de un sorteo de 60 televisores Led Samsung de 55 pulgadas, 100 Play Station 4 y 250 celulares Motorola E5 16GB. Este correo además intenta engañar que su origen es del dominio "meteo Chile.cl" perteneciente a la Dirección Meteorológica de Chile, considerar que el correo no proviene de dicho dominio.

### Indicadores de compromisos

#### Url's:

[http://scotiablakclpersonas1bancenlinea.mjzerin\[.\]com/](http://scotiablakclpersonas1bancenlinea.mjzerin[.]com/)

[http://pyramidskateshop\[.\]com/54747633207622423753336611550529](http://pyramidskateshop[.]com/54747633207622423753336611550529)

[https://mr-thompson-science\[.\]com/scotiablakclpersonas1bancenlinea/562YSV/login/l3OMW/personas//](https://mr-thompson-science[.]com/scotiablakclpersonas1bancenlinea/562YSV/login/l3OMW/personas//)

**Smtip Host**

[23.163.0.41]  
[23.152.0.42]  
[185.243.114.82]  
[23.163.0.43]  
[23.152.0.37]  
[192.52.167.86]  
[185.99.133.203]  
[193.29.58.134]  
[guiltmature.pw]  
[192.169.7.75]  
[192.169.7.84]  
[23.152.0.38]  
[192.169.7.29]  
[46.159.70.196]

**From: (Original)**

@vps.server.com

**Subject:**

Felicidades Ganastes un Bono

## Imagen



Banco Scotiabank <premios-lsrxrdy@meteochile.cl> | cliente

**Felicidades Ganastes un Bono**

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



### Felicidades Ganastes.

Estimado : **CLIENTE**

Para eso que tienes pensado **GANASTE** un abono en tu línea de crédito de \$ 999.999, usalo en lo mejor que te parezca. Al aumentar el cupo en tu Línea de Crédito ingresaste automáticamente también al sorteo de 60 televisores LED Samsung de 55 pulgadas , 100 PLAY STATION 4 , 250 Motorola E5 16GB.  
**Quiero Aprobar el abono CODIGO ABONO [N.82.940]**

Recuerde que tiene un plazo de 42 horas después de haber recibido este mensaje para **APROBAR EL ABONO**, finalizando el tiempo establecido se anulará el premio Otorgado. **CODIGO ABONO [N.82.940]** .

2019. S.A.C.I Scotiabank Chile. Todos los Derechos Reservados



[← Ir al Portal Scotiabank](#)

## Ingreso Personas

RUT

Clave

ver clave

[Olvidé mi Clave](#)

[Ingresar a Scotiaweb](#)

[Soy Cliente, pero no tengo clave](#)

### Scotiabank informa


Respecto a falsos llamados telefónicos realizados por delincuentes para obtener tu dinero, te recomendamos seguir los siguientes consejos de Seguridad


[Ver más información](#)




### ¿Necesita Ayuda?

 Centro de Contacto  
**914 7946 426**  
**+44 (2) 523 78 850**

 Emergencias Bancarias

 Recomendaciones de Seguridad

 Solicitud de Clave ScotiaWeb

 Canales de Atención

Búscanos en:




[> Descargo de Responsabilidad](#) | [> Código de Conducta y Buenas Prácticas de Bancos e Instituciones Financieras](#)  
Infórmese sobre el límite de garantía estatal a los depósitos en su banco o en [www.sbf.cl](#) | [> Defensoría del Cliente](#)  
[> Manejo de Información de Interés para el Mercado](#) | [> Prepaagos y Refinanciamiento de Créditos](#)

## Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

## Contactos

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

 + (562) 24863850

 @CSIRTGOB

 <https://www.linkedin.com/company/csirt-gob>