

Alerta de seguridad cibernética	8FPH20-00266-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Julio de 2020
Última revisión	13 de Julio de 2020

## 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 afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del Banco Scotiabank.

El atacante intenta persuadir a las potenciales víctimas para utilizar un enlace en el cuerpo del correo. El mensaje del correo, el que imita una campaña del banco, invita a los usuarios a informarse sobre una promoción que le permitirá cancelar las deudas de tres cuotas a final de año.

Al seleccionar el botón para ingresar al Banco Scotiabank, el usuario es dirigido a un sitio falso del banco, donde se expone al robo de sus credenciales.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

### Urls Redirecciones:

hxxp://vitriuesdemetz[.]com/key[.]php

hxxp://elec-brico[.]fr/click[.]php

### Urls sitio falso:

hxxps://scotiachile[.]ga/scotiabank/portal/Pre-login/www[.]scotiabank[.]cl

### Sender

www-data[.]gmail[.]com

### Smtip Host

[103.248.146.11]

### Asunto

Quedate en Casa - Conoce todas las alternativas que ofrecemos

## Otros antecedentes

## URL Body SHA-256

55b167bd6e846c6fc82a197efbd6b946100bdb0f19ae713d01b3e876a4e417a0

## Certificado Digital

Fecha Valido : 12-07-2020  
Fecha Termino : 10-10-2020  
Emitido : Let's Encrypt Authority X3

## Datos Alojamiento

IP : 178.159.36.76  
Número de sistema autónomo (AS) : AS 48666  
Etiqueta del sistema autónomo : MAROSNET Telecommunication Company LLC  
País : Rusia  
Registrador : RIPE NCC

## Datos del Dominio

Nombre de dominio : SCOTIACHILE[.]GA  
Información del registrador : Gabon TLD B.V.  
Correo electrónico : abuse@freenom.com  
Servidores de nombres : NS01.FREENOM.COM  
NS02.FREENOM.COM  
NS03.FREENOM.COM  
NS04.FREENOM.COM




## Imagen del mensaje

De: scotiabankchile@enlinea.cl

Para:

CC:

Asunto: Quédate en Casa - Conoce todas las alternativas que ofrecemos - ( 532950998749 )



QUÉDATE EN CASA


DE ESTA SALIMOS,  
SIN TENER QUE SALIR.  
#QuédateEnCasa

Participa por tus deudas y las cancelas  
en los próximos 3 meses del año

**Tu tranquilidad es nuestro compromiso**


Conoce todas las alternativas que ofrecemos

**Aquí**



Quédate en casa


**Acciones para ayudar**  
a clientes y empleados  
#MásCercaQueNunca




Quédate en casa



**Nuestros seguros cubren COVID-19\***

**Conoce más**



Más información en [Scotiabank.cl](https://www.scotiabank.cl)

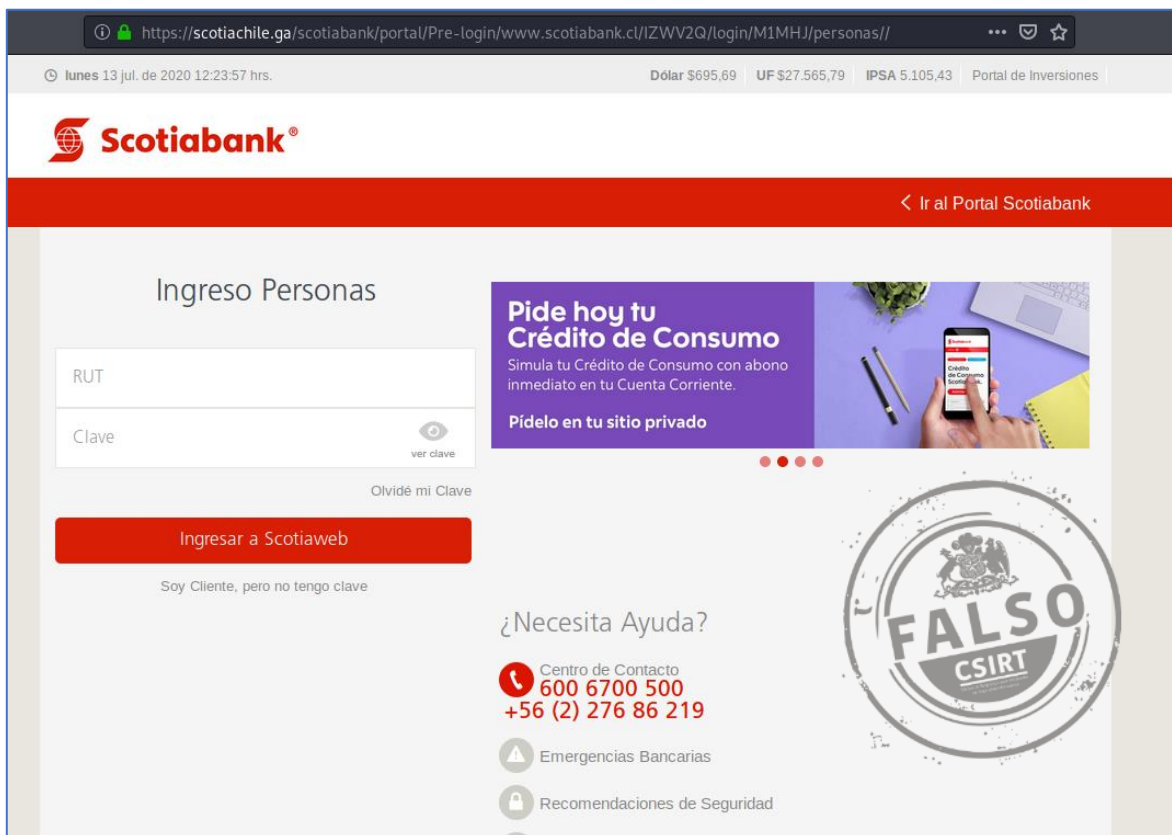
 **Porque tu seguridad es lo primero,**  
te recomendamos seguir estos consejos

-  **Nunca** mantengas tu antivirus desactualizado.
-  **Nunca** te llamaremos para pedir tus claves por ningún motivo.

6006700 500 [scotiabank.cl](https://www.scotiabank.cl)

Has recibido este correo porque figura como el E-mail de tu cuenta Scotiabank. Para modificarlo contactate con tu ejecutiva o visita una de nuestras sucursales. Informese sobre la garantía estatal de los depósitos en subancho o en [www.cmfchile.cl](https://www.cmfchile.cl) 2020 Scotiabank.com Todos los derechos reservados.

## Imagen del sitio



## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.
- Visualizar los sitios web que se ingresen sean los oficiales.
-