

Alerta de seguridad informática	8FPH20-00082-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de Enero de 2019
Última revisión	03 de Enero 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 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), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Scotiabank para seleccionar un hipervínculo que los direcciona a un sitio semejante al del Banco. Para ello, el atacante utiliza un mensaje indicando que existe una transferencia de fondos retenida y así convencer a la víctima de seleccionar el enlace.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

## Indicadores de compromisos

### Url's:

[https://www1\[.\]acceso.scotia.cl\[.\]no-cache\[.\]info](https://www1[.]acceso.scotia.cl[.]no-cache[.]info)

### Sender

www-data@gmail[.]com

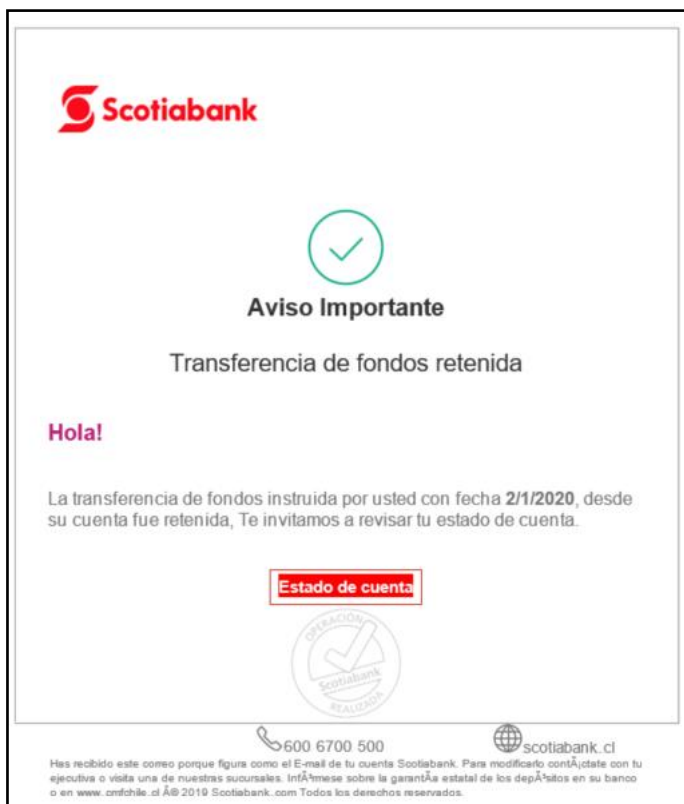
### Smtip Host

103[.]248[.]146[.]2

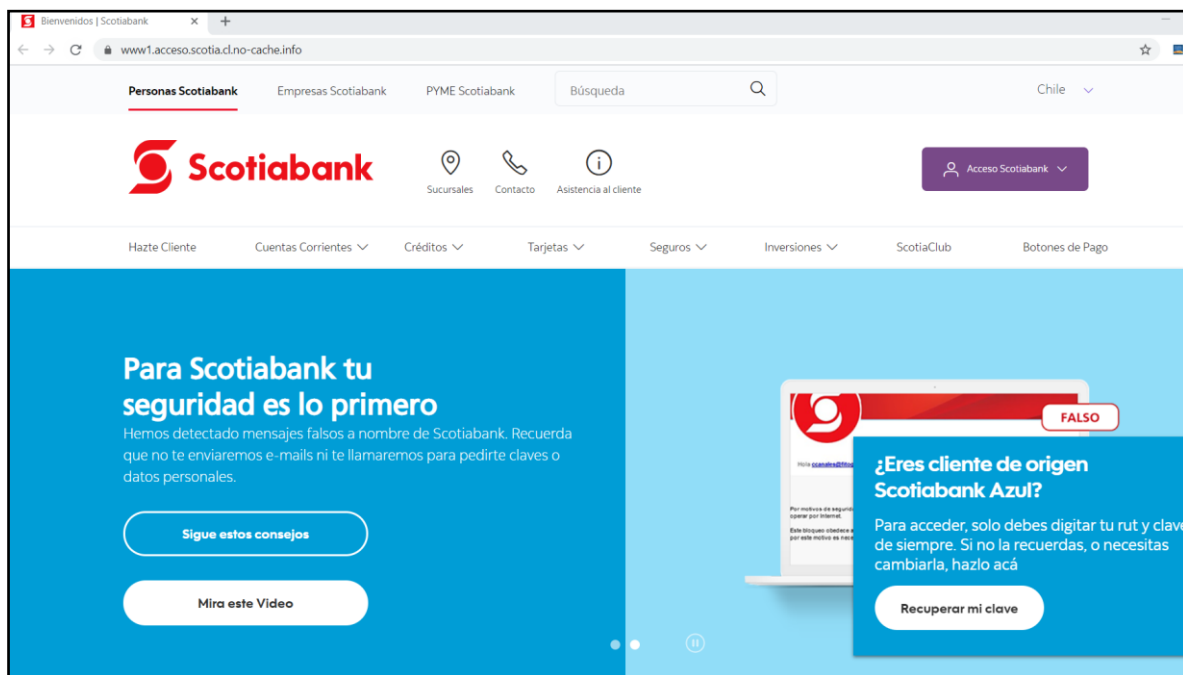
### Subject:

Aviso de Transferencia

## Imagen Phishing Correo



## Imagen Sitio Web



## 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
- Visualizar los sitios web que se ingresen que sean los oficiales