Alerta de seguridad informática	8FPH-00076-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Diciembre de 2019
Última revisión	11 de Diciembre 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 afecta 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.

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, los atacantes utilizan diversos mensajes en el cuerpo del correo para convencer a la víctima de seleccionar el enlace, cómo por ejemplo:

- Que su cuenta se le descontó $300.000 pesos por un incumplimiento de un pago
- Que la cuenta fue suspendida por no realizar un pago de impuestos
- Que se le descontó $450.000 pesos por un error en los sistemas
- Que su tarjeta de crédito por realizar una operación sospechosa se procedió a su bloqueo

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

https[:]//elemfsent[.]com/scotiablakclpersonas1bancenlinea

https[:]//pictureframingdroitwich[.]com/scotiablakclpersonaslbancenlinea

Smtp Host

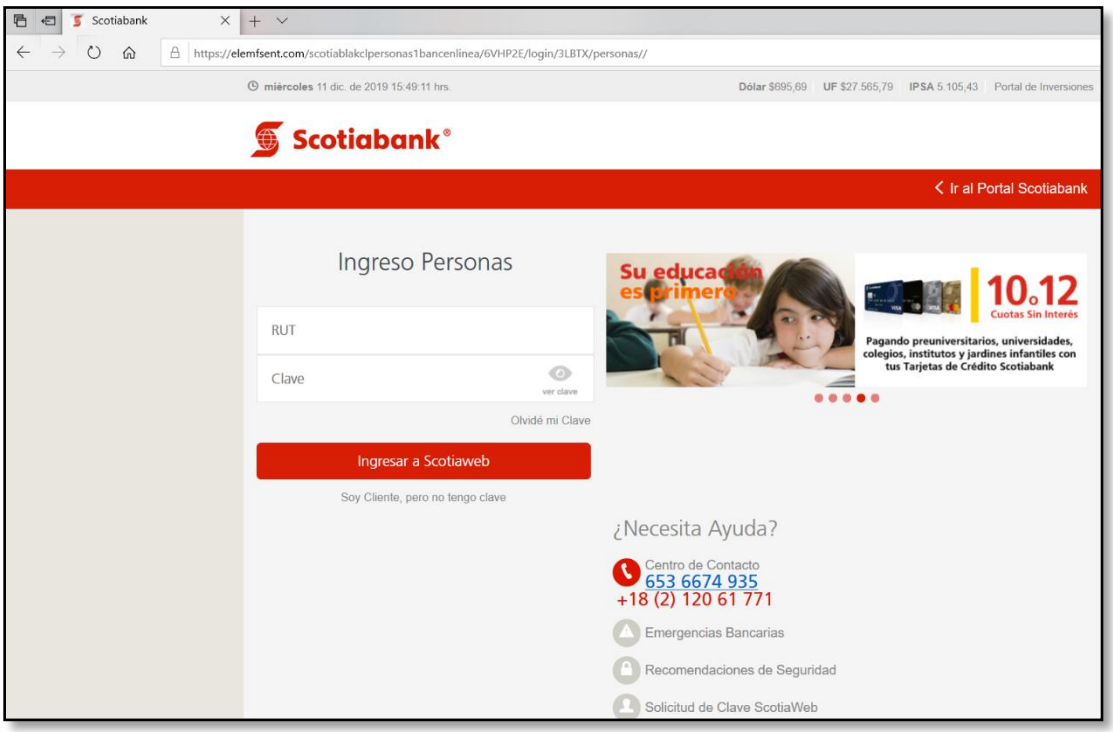
[176[.]31[.]193[.]51]
[185[.]174[.]173[.]29]
[185[.]174[.]173[.]42]
[185[.]174[.]173[.]84]
[185[.]174[.]173[.]86]
[185[.]174[.]173[.]88]
[185[.]174[.]173[.]131]
[185[.]174[.]172[.]234]
[185[.]174[.]172[.]239]
[185[.]174[.]172[.]241]

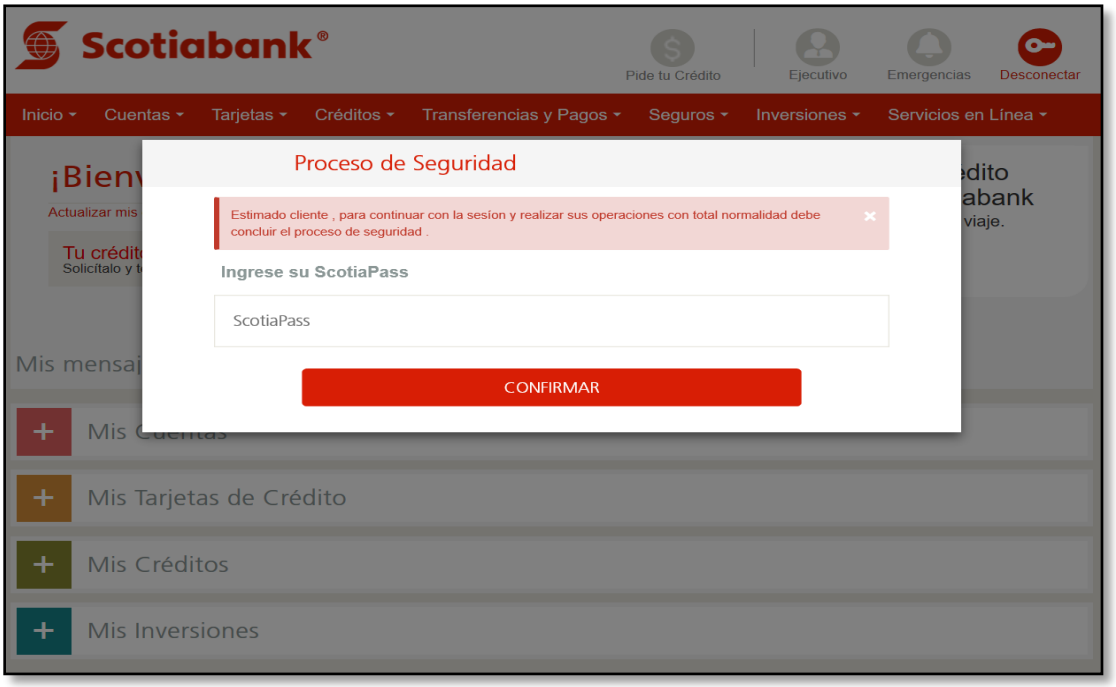
Subject:

Verificar Operación
Descuento por deuda
Retencion por deuda
Boqueo por Impuesto
Error de descuento
Deuda Pendiente
Informe de Operación
Impuesto no Pagado
Operacion Bloqueada
Descuento Cancelado
Detalle descuento por error
Movimiento Ilegal

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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.11 18:12:36 -03'00'