Alerta de seguridad cibernética	8FPH20-00164-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Abril de 2020
Última revisión	09 de Abril 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 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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico falso que aparenta provenir del Banco Scotiabank.

El mensaje del correo informa a quien lo recibe que se realizó un descuento de $ 221.000 pesos, de manera automática, desde su cuenta por incumplimiento de un pago. El atacante dispone un enlace para supuestamente obtener más detalle del descuento. Si una persona selecciona el enlace, es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales bancarias.

CSIRT agradece la información prestada por Rodrigo Ostolaza a través de Twitter para alertar sobre esta campaña de phishing, y alienta a quienes encuentren otras campañas similares a reportar la información a través de nuestro formulario en el sitio web www.csirt.gob.cl o al teléfono +(562) 2486 3850, el que está disponible las 24 horas para atención.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls Redirecciones:
https[:]//overallcolorful[.]com/945d94534f2f5dc28be499d0675f5164

Urls sitio falso:
http[://scotia.1526.online-cl[.]live/1586439240/login/personas

Smtp Host
[164.68.107.57]
[5.182.211.102]
[164.68.116.247]

Sender
apache@86974.ip-ns[.]net
apache@86973.ip-ns[.]net
apache@info[.]cl

Asunto
Detalle por retención
Deuda cancelada
Retención por deuda

IMAGEN DEL MENSAJE

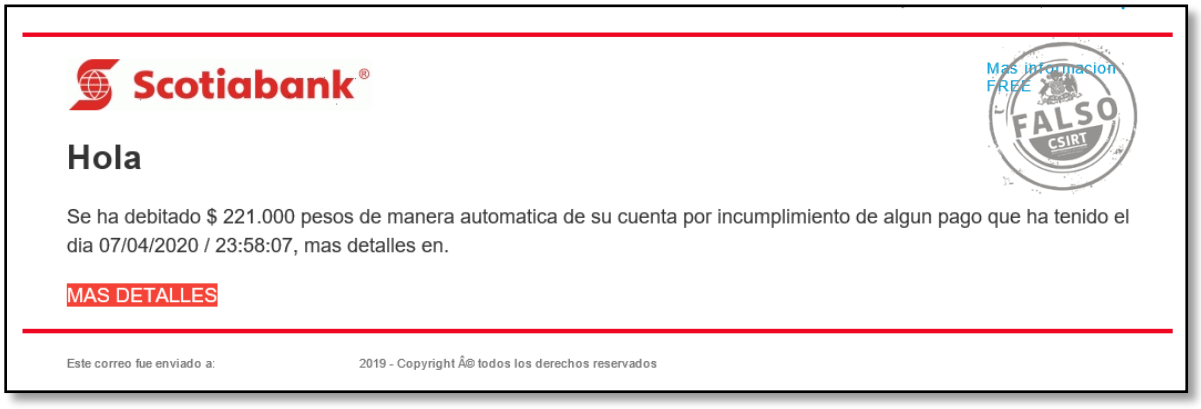
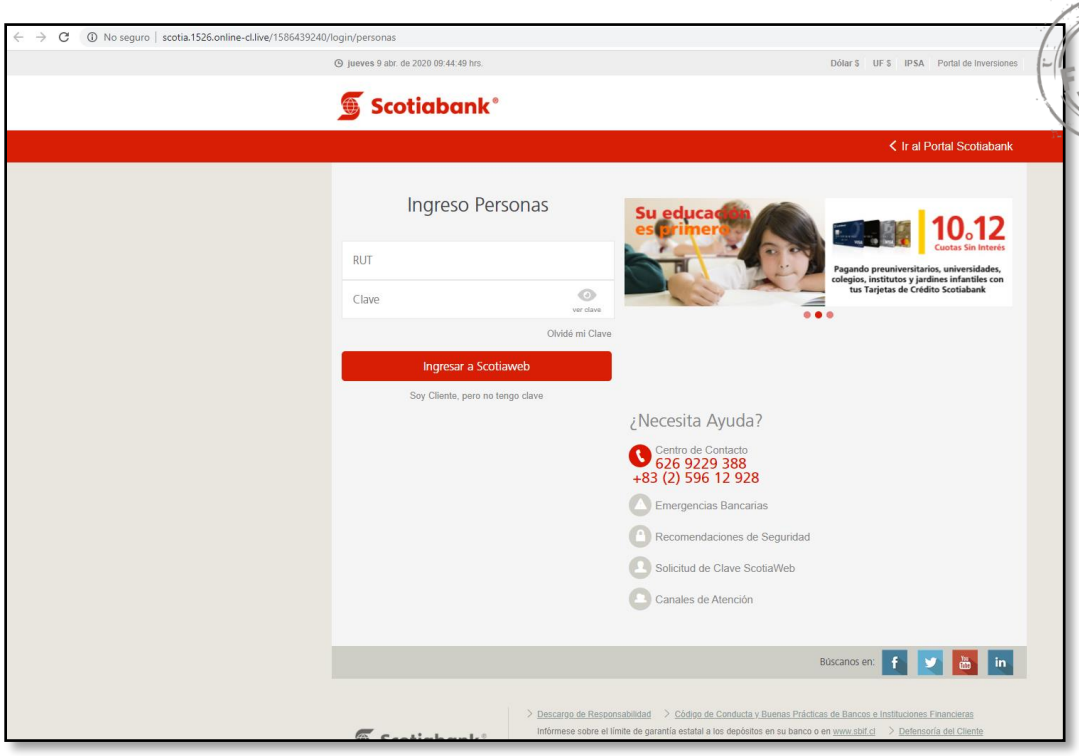


IMAGEN DEL SITIO



RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen
- Prestar atención en los detalles de los mensajes o redes sociales
- Desconfiar de promociones que no se encuentren en los canales oficiales
- Siempre visitar los canales de comunicaciones oficiales
- 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 sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.09 12:34:16 -04'00'