Alerta de seguridad cibernética	8FPH20-00182-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 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, que aparenta provenir del Banco Scotiabank.

El mensaje intenta persuadir a las personas para utilizar un enlace malicioso adjunto en el cuerpo del correo.

Quien recibe el correo es informado sobre la detección de un inconveniente con su dispositivo de seguridad, por lo que se requiere su sincronización de forma inmediata. El mensaje advierte de un tiempo límite para realizar la acción -48 horas desde recibido el correo- de lo contrario la cuenta podría ser bloqueada, lo que podría generar presión en la decisión de la víctima para ingresar a los enlaces disponibles en el correo para realizar la gestión de sincronizar el dispositivo.

Si la persona utiliza el enlace, es redirigido a un sitio semejante al del banco donde se expone al robo de sus credenciales bancarias.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls Redirecciones:
http[:]//niudimai[.]com/817d35dd266a19abc6c3f23bcdd04f36

Urls sitio falso:
https[:]//scotiapersonascl[.]scopsonas[.]com/1587145421/login/personas

Smtp Host
[54.37.45.124]
[10.13.138.144]
[54.37.239.19]
[54.38.133.169]

Sender
apache[@]86899[.]ip-ns[.]net
apache[@]86988[.]ip-ns[.]net
apache[@]87078[.]ip-ns[.]net
apache[@]87069[.]ip-ns[.]net
apache[@]87070[.]ip-ns[.]net
apache[@]87073[.]ip-ns[.]net
apache[@]86902[.]ip-ns[.]net

Asunto
Error en su Dispositivo

IMAGEN DEL MENSAJE

Aviso Importante

Estimado Cliente: [redacted]

Le informamos que nuestros sistemas han detectado un inconveniente con su dispositivo de seguridad, por lo que se requiere sincronizarlo de manera inmediata. Este procedimiento solo sera solicitado por unica vez, ya que garantiza la proteccion de sus datos y no sera necesario solicitarla nuevamente.

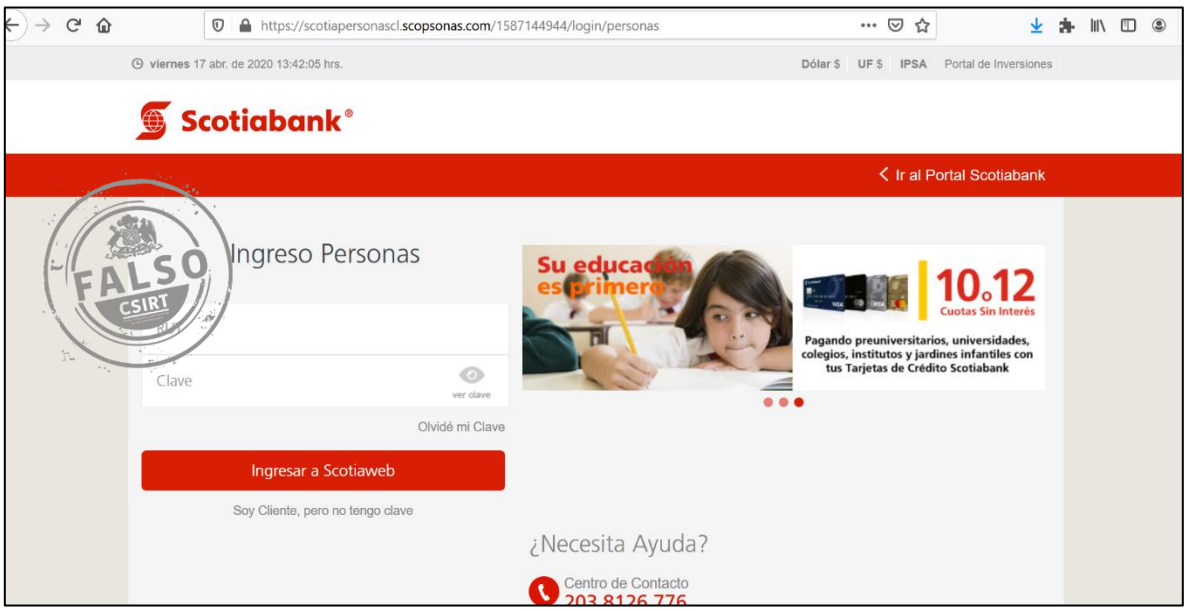
Estado de Dispositivo	**No Sincronizado**

Sincronizar Dispositivo

Recuerde que solo tiene 48 horas despues de recibir este email para realizar dicho proceso, de lo contrario su cuenta sera bloqueada y tendra que acercarse a la sucursal mas cercana para solicitar una nueva tarjeta.

Has recibido este correo porque figura como el E-mail de tu cuenta Scotiabank. Para modificarlo contÃ¡ctate con tu ejecutiva o visita una de nuestras sucursales. InfÃ³rmese sobre la garantÃa estatal de los depÃ³sitos en su banco o en www . cmfchile. cl Â© 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.17 18:33:55 -04'00'