Alerta de seguridad informática	8FPH20-00142-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Marzo de 2020
Última revisión	24 de Marzo 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 aparente provenir del Banco BCI.

El mensaje del correo ofrece el aumento del cupo de la línea de crédito y que automáticamente participaran en el sorteo de 60 televisores LED Samsung de 55”, 100 PLAY STATION 4 y 250 Motorola E5 16GB. Si una persona selecciona el enlace será dirigido a un sitio semejante al 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:
http[:]//www[.]bciportal1[.]ns1[.]name/

Urls sitio falso:
https[:]//personasinfo[.]xyz/sRVffTNyi0VWdOZeY/cl/bci/aplicaciones/contenido/personas

Smtp Host
64[.]44[.]34[.]130
64[.]44[.]34[.]13

Sender
admin[@]marathon[.]org

Asunto
Aprueba tu cupo por $ 500,000 por todo marzo

IMAGEN DEL MENSAJE

De: Bci <enviodigital@eeccvirtual.site>
Para:
CC:
Asunto: Aprueba tu cupo por $ 500,000 por todo marzo

BANCO BCI

Si no visualiza el correo completo haga clic en Mostrar Contenido Bloqueado

Estimado(a) cliente

No te quedes **sin efectivo.**

Para eso que tienes pensado tienes un cupo en tu linea de credito de $ 500,000, usalo en lo mejor que te parezca. Al aumentar el cupo en tu Linea de Credito ingresaste automaticamente tambien al sorteo de 60 televisores LED Samsung de 55' - 100 PLAY STATION 4 - 250 Motorola E5 16GB

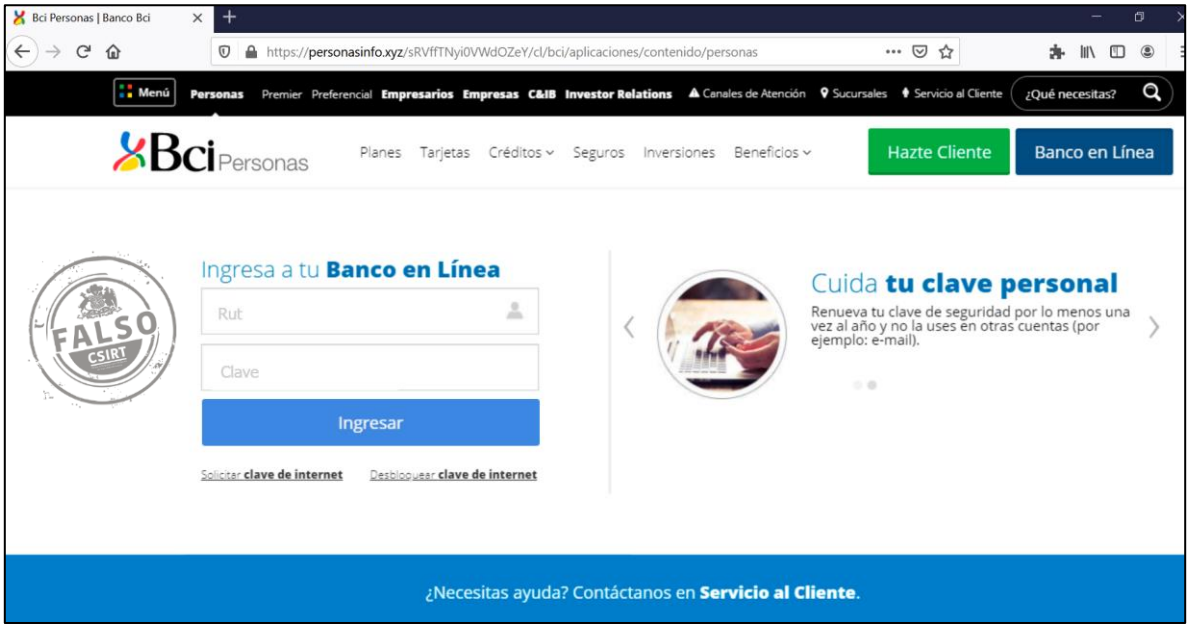
Promocion todo este mes de marzo

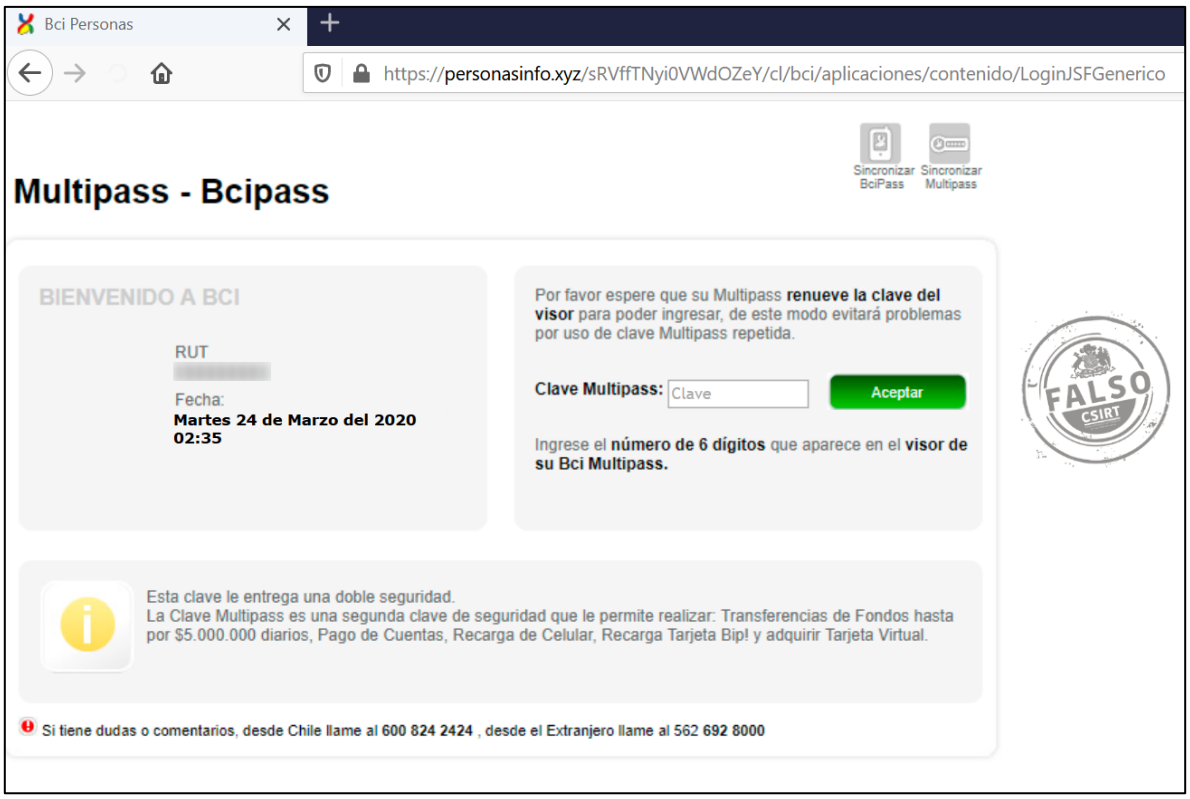
Para Aprobar su abono ingrese al siguiente link

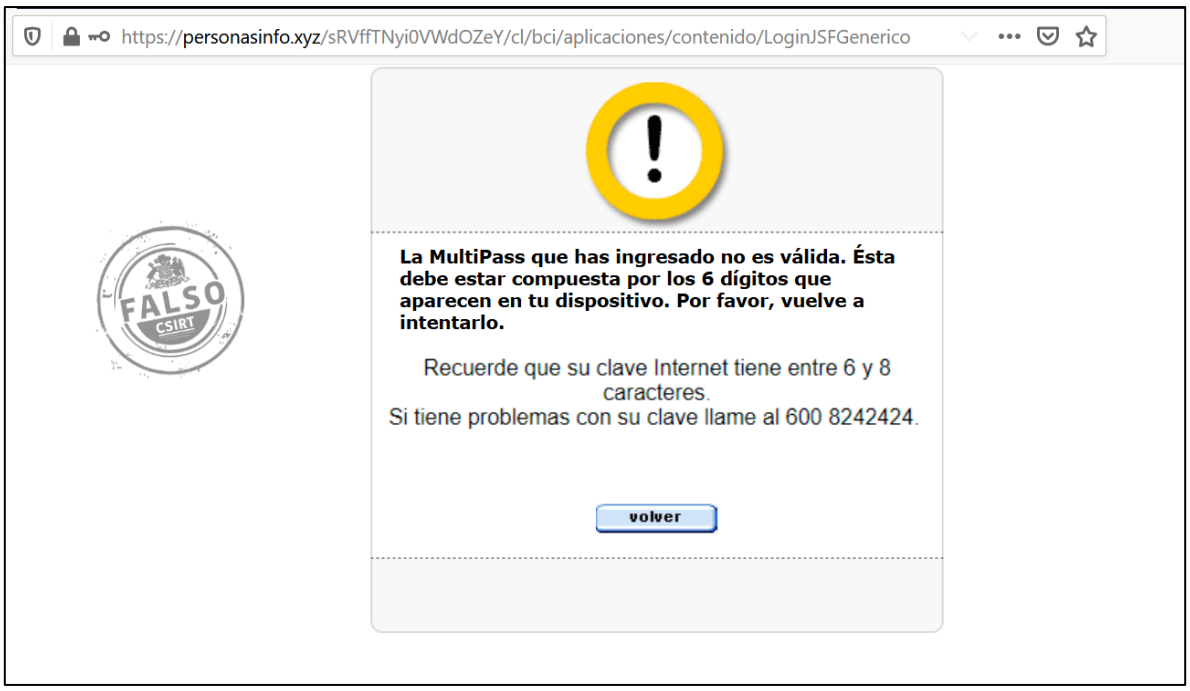
Aprobar Linea de Credito

Las tildes fueron omitidas intencionalmente
Este correo electronico se le envio a
Casa Matriz: Av. El Golf 125, Santiago de Chile
Informese sobre la garantia estatal de los depositos en su banco o en www.sbif.cl
2019 Banco Bci. Todos los Derechos Reservados.

FALSO CSIRT


Bci Personas | Banco Bci
https://personasinfo.xyz/sRVffTNyi0VWdOZeY/cl/bci/aplicaciones/contenido/personas
Menú
Personas
Premier
Preferencial
Empresarios
Empresas
C&IB
Investor Relations
Canales de Atención
Sucursales
Servicio al Cliente
¿Qué necesitas?
Bci Personas
Planes
Tarjetas
Créditos
Seguros
Inversiones
Beneficios
Hazte Cliente
Banco en Línea
FALSO
CSIRT
Ingresa a tu Banco en Línea
Rut
Clave
Ingresar
Solicitar clave de internet
Desbloquear clave de internet
Cuida tu clave personal
Renueva tu clave de seguridad por lo menos una vez al año y no la uses en otras cuentas (por ejemplo: e-mail).
¿Necesitas ayuda? Contáctanos en Servicio al Cliente.


Bci Personas
https://personasinfo.xyz/sRVffTNyi0VWdOZeY/cl/bci/aplicaciones/contenido/LoginJSFGenerico
Sincronizar BciPass
Sincronizar Multipass
Multipass - Bcipass
BIENVENIDO A BCI
RUT
Fecha:
Martes 24 de Marzo del 2020
02:35
Por favor espere que su Multipass renueve la clave del visor para poder ingresar, de este modo evitará problemas por uso de clave Multipass repetida.
Clave Multipass:
Clave
Aceptar
Ingrese el número de 6 dígitos que aparece en el visor de su Bci Multipass.
FALSO
CSIRT
Esta clave le entrega una doble seguridad.
La Clave Multipass es una segunda clave de seguridad que le permite realizar: Transferencias de Fondos hasta por $5.000.000 diarios, Pago de Cuentas, Recarga de Celular, Recarga Tarjeta Bip! y adquirir Tarjeta Virtual.
Si tiene dudas o comentarios, desde Chile llame al 600 824 2424 , desde el Extranjero llame al 562 692 8000



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 sean los oficiales.

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.24 18:23:31 -03'00'