Alerta de seguridad informática	**8FFR-00092-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**15 de Octubre de 2019**
Última revisión	**15 de Octubre 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 fraude 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 fraude, 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 la activación de una serie de portales bancarios fraudulentos asociado a una IP que redirige a sitios que suplantan a 10 bancos que operan en Chile, con el propósito de robar credenciales de usuarios de las entidades:

- Banco Scotiabank
- Banco Chile
- Banco Estado
- Banco Falabella
- Banco Bci
- Banco Bice
- Banco Itau
- Banco Santander
- Banco Security
- Banco Ripley

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s

URL Sitio Clonado:
http[://]104[.]36[.]229[.]160/0ita1/
http[://]104[.]36[.]229[.]160/0santa1/
http[://]104[.]36[.]229[.]160/0rip1/
http[://]104[.]36[.]229[.]160/0office1/
http[://]104[.]36[.]229[.]160/0bs1/
http[://]104[.]36[.]229[.]160/0be1/
http[://]104[.]36[.]229[.]160/0bci1/
http[://]104[.]36[.]229[.]160/0fala1/
http[://]104[.]36[.]229[.]160/0bbva1/
http[://]104[.]36[.]229[.]160/0bice1/
http[://]104[.]36[.]229[.]160/0bchile1/

IP´s

104[.]36[.]229[.]160

IP address
<< 104.36.229.160 >>

Block start	104.36.224.0
End of block	104.36.231.255
Block size	2048 Domains in block
Block name	VWEB-6
AS number	395092
Parent block	104.0.0.0 - 104.255.255.255
Organization	Versaweb, LLC
City	Las Vegas
Region/State	Nevada
Country	US , United States
Reg. date	2014-06-05
Host name	no record in reverse zone
Domains	not found

Ilustración 1 Dirección Ip de Sitio Fraudulento a la Banca Chilena

Localización

Las Vegas Nevada, United States

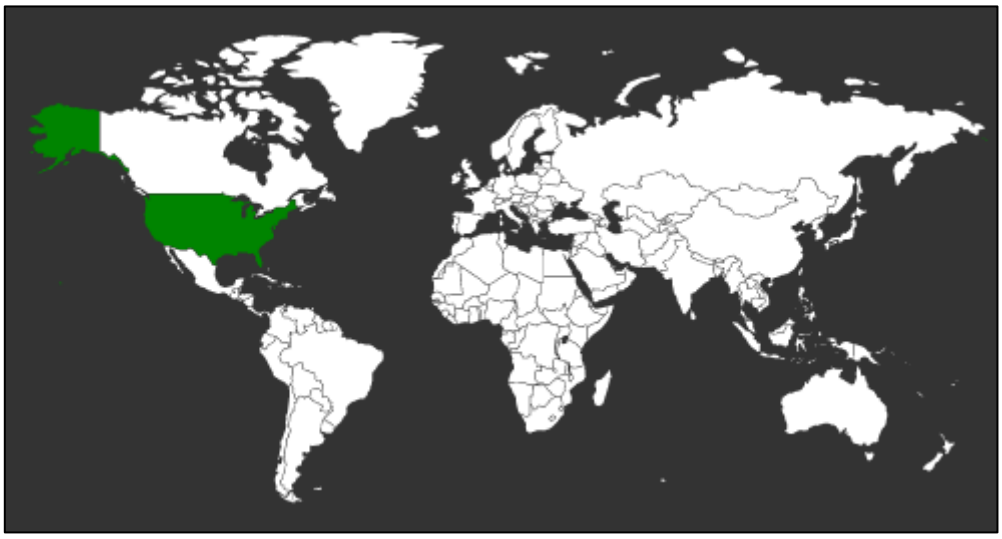
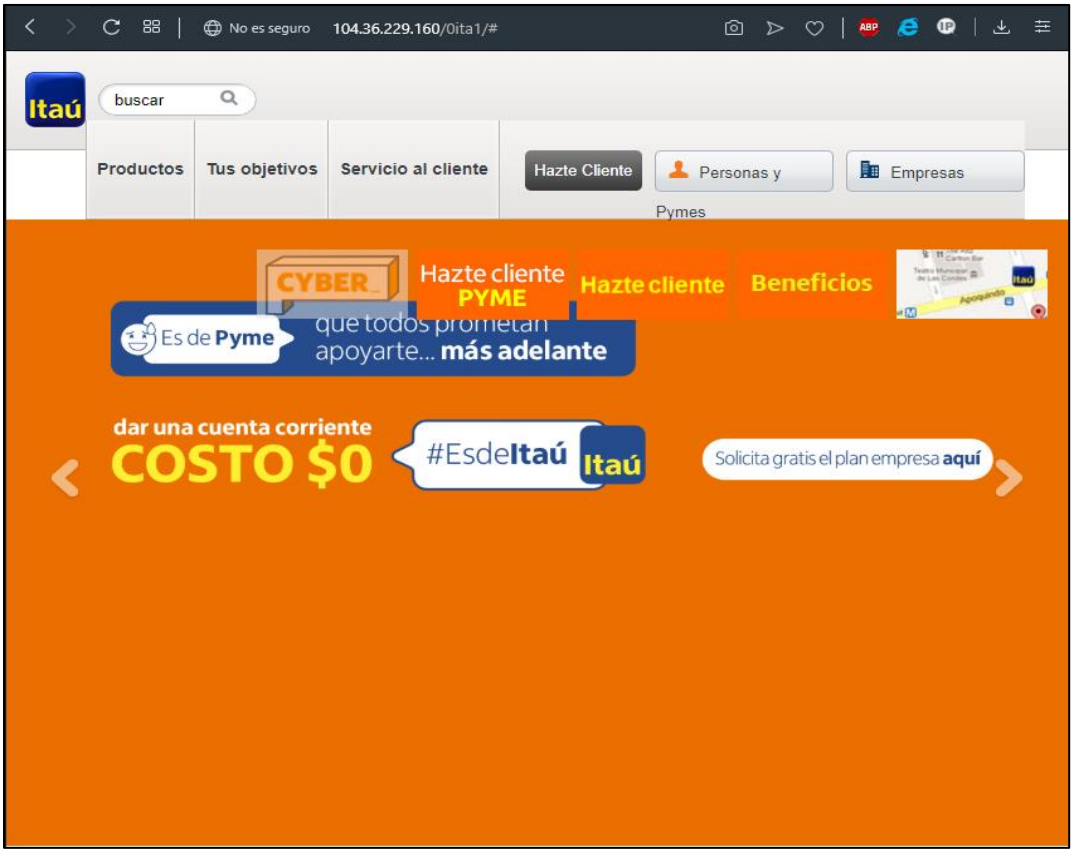
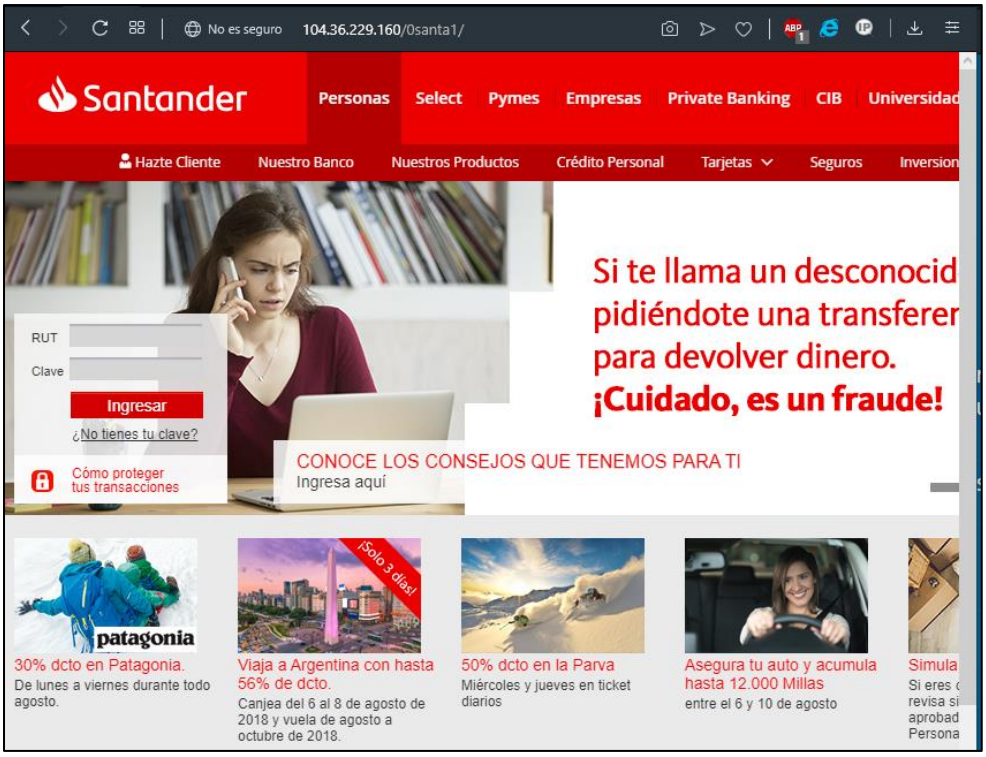
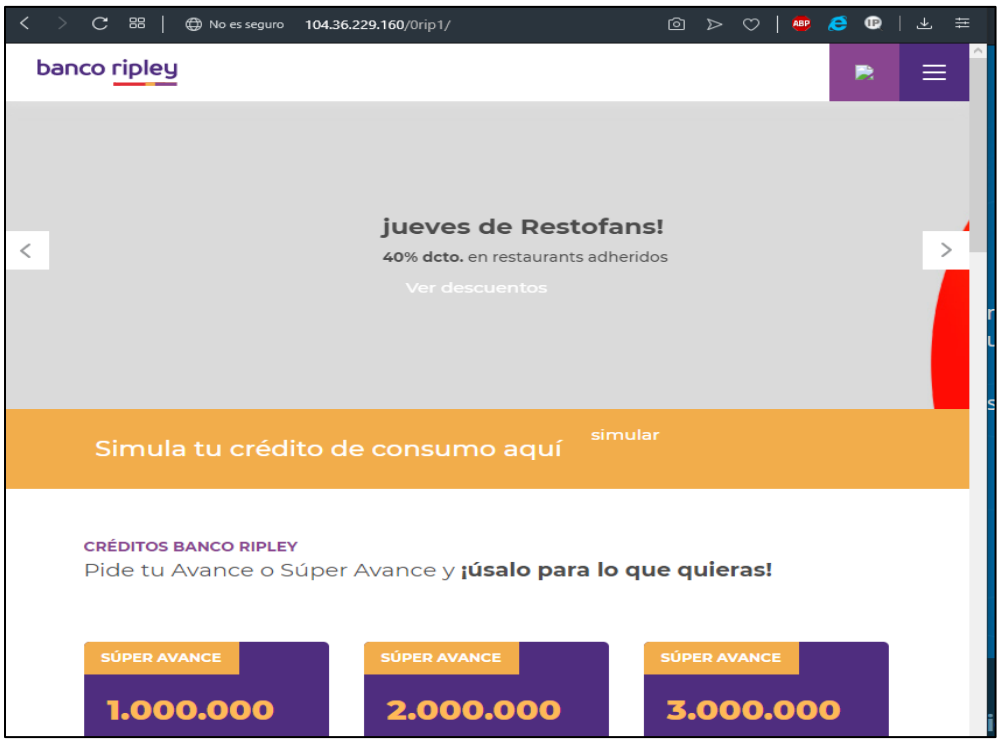
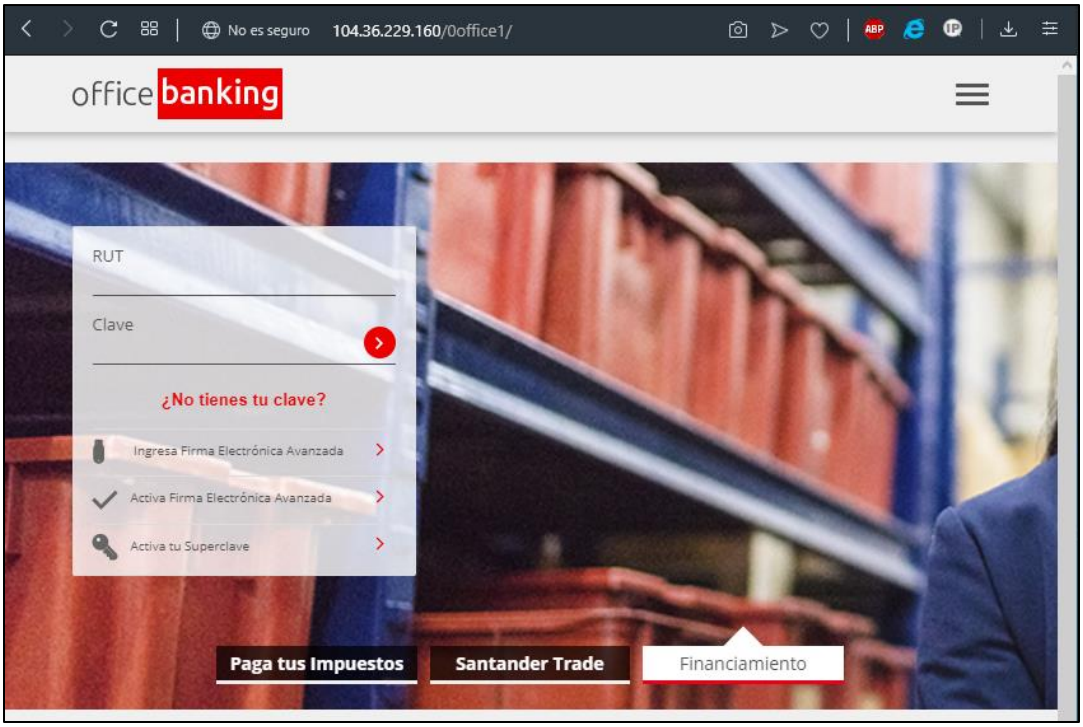


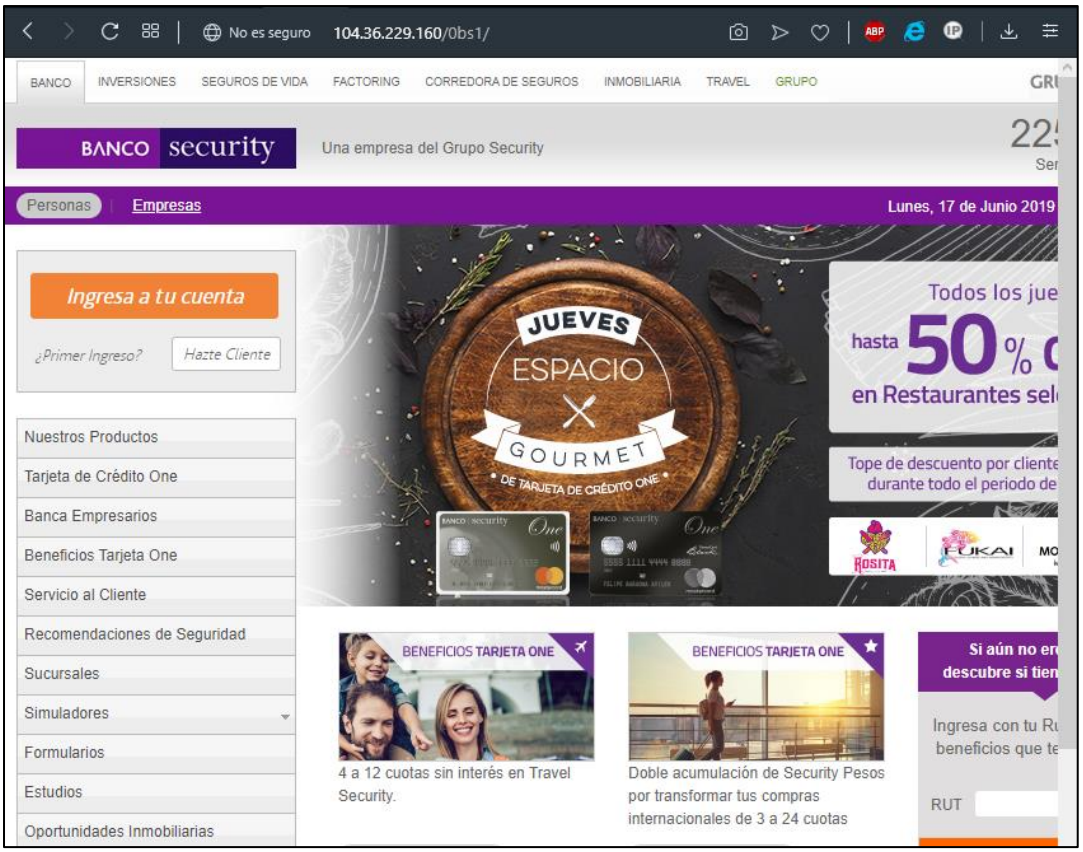
Imagen de los Sitios

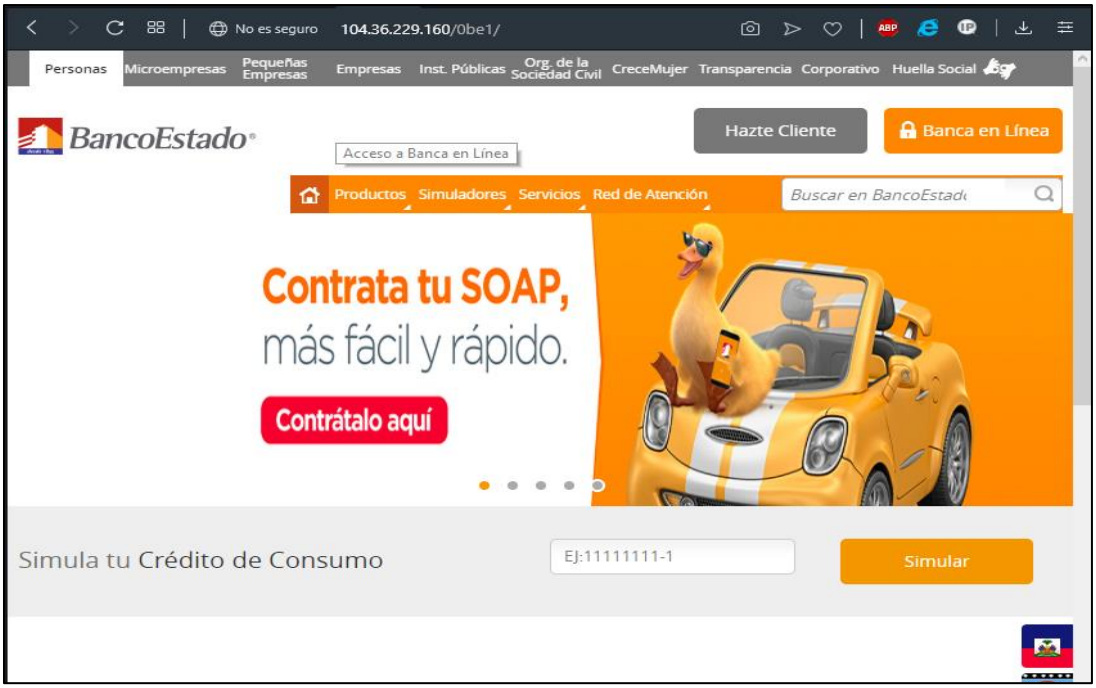


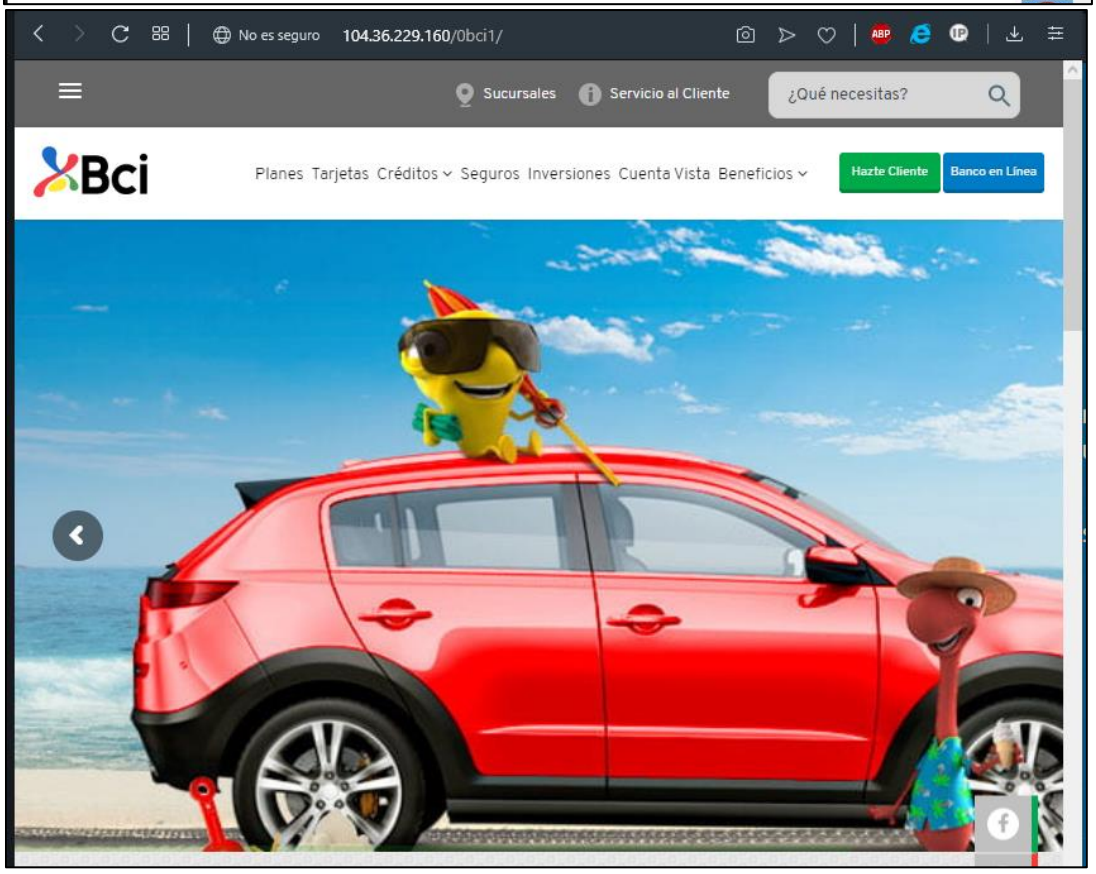

No es seguro
104.36.229.160/0santa1/
Santander
Personas
Select
Pymes
Empresas
Private Banking
CIB
Universidad
Hazte Cliente
Nuestro Banco
Nuestros Productos
Crédito Personal
Tarjetas
Seguros
Inversion
RUT
Clave
Ingresar
¿No tienes tu clave?
Cómo proteger tus transacciones
Si te llama un desconocid
pidiéndote una transferer
para devolver dinero.
¡Cuidado, es un fraude!
CONOCE LOS CONSEJOS QUE TENEMOS PARA TI
Ingresa aquí
patagonia
30% dcto en Patagonia.
De lunes a viernes durante todo agosto.
¡Solo 3 días!
Viaja a Argentina con hasta 56% de dcto.
Canjea del 6 al 8 de agosto de 2018 y vuela de agosto a octubre de 2018.
50% dcto en la Parva
Miércoles y jueves en ticket diarios
Asegura tu auto y acumula hasta 12.000 Millas
entre el 6 y 10 de agosto
Simula


No es seguro
104.36.229.160/0rip1/
banco ripley
jueves de Restofans!
40% dcto. en restaurants adheridos
Ver descuentos
Simula tu crédito de consumo aquí
simular
CRÉDITOS BANCO RIPLEY
Pide tu Avance o Súper Avance y ¡úsalo para lo que quieras!
SÚPER AVANCE
1.000.000
SÚPER AVANCE
2.000.000
SÚPER AVANCE
3.000.000

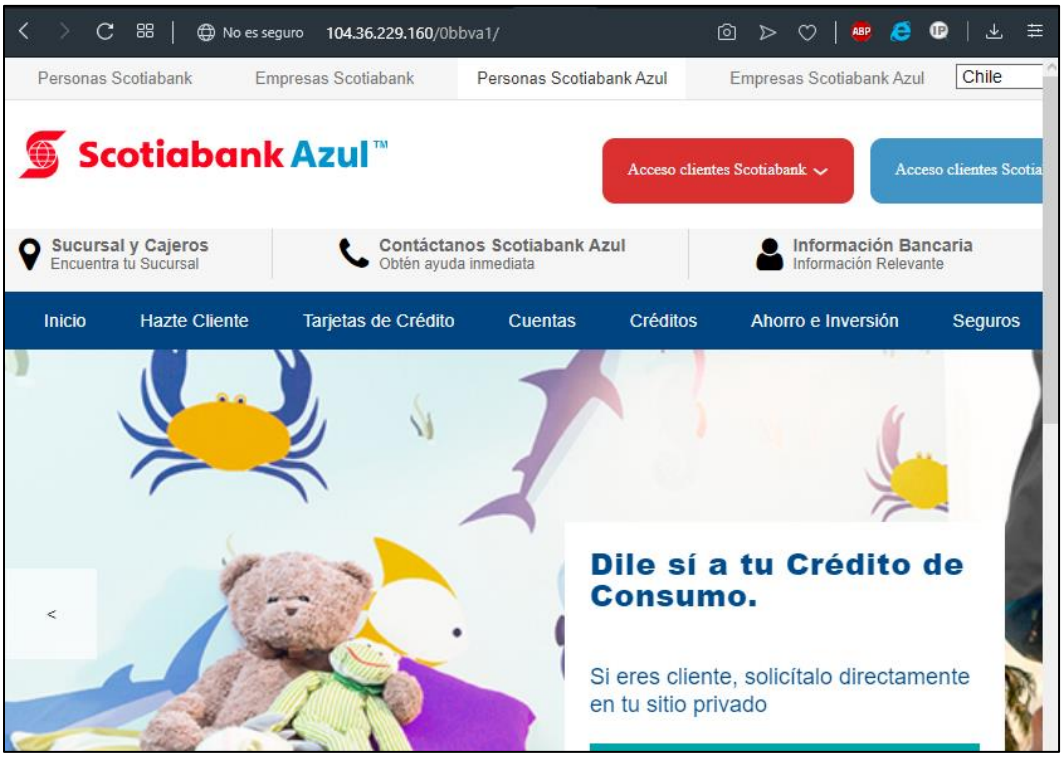

No es seguro
104.36.229.160/0office1/
office banking
RUT
Clave
¿No tienes tu clave?
Ingresa Firma Electrónica Avanzada
Activa Firma Electrónica Avanzada
Activa tu Superclave
Paga tus Impuestos
Santander Trade
Financiamiento

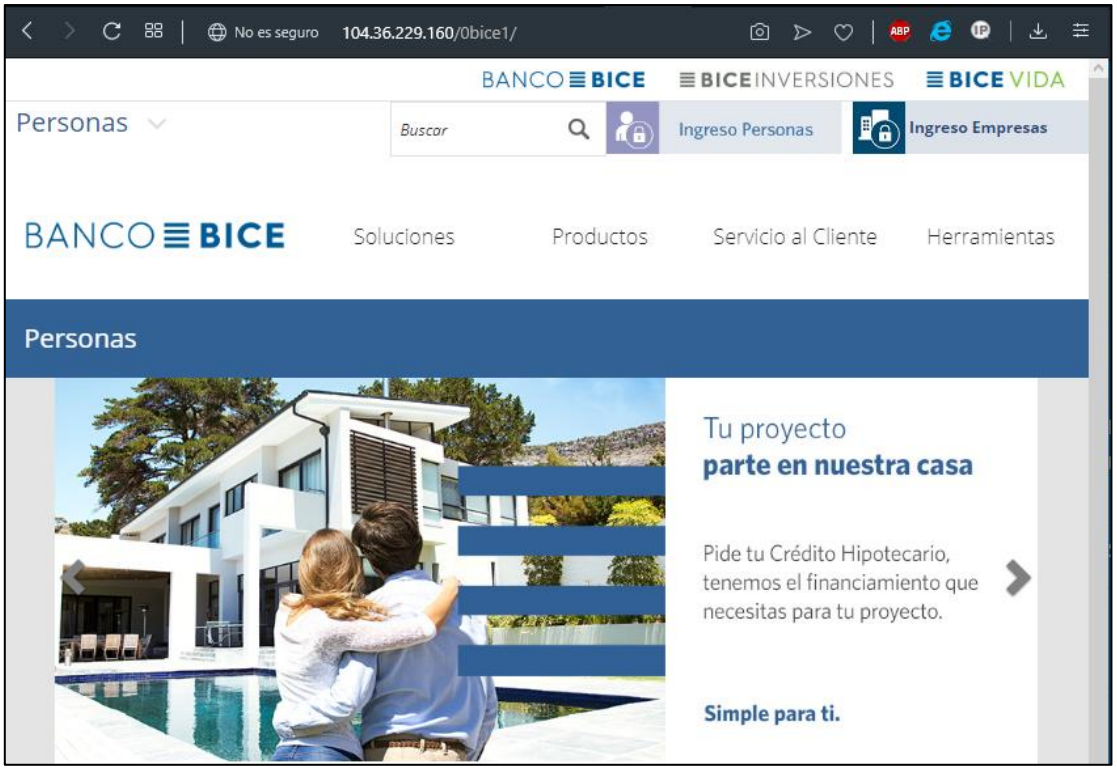

No es seguro
104.36.229.160/0bs1/
BANCO
INVERSIONES
SEGUROS DE VIDA
FACTORING
CORREDORA DE SEGUROS
INMOBILIARIA
TRAVEL
GRUPO
BANCO security
Una empresa del Grupo Security
Personas
Empresas
Lunes, 17 de Junio 2019
Ingresa a tu cuenta
¿Primer Ingreso?
Hazte Cliente
Nuestros Productos
Tarjeta de Crédito One
Banca Empresarios
Beneficios Tarjeta One
Servicio al Cliente
Recomendaciones de Seguridad
Sucursales
Simuladores
Formularios
Estudios
Oportunidades Inmobiliarias
JUEVES
ESPACIO
GOURMET
DE TARJETA DE CRÉDITO ONE
Todos los jue
hasta 50 %
en Restaurantes sel
Tope de descuento por cliente
durante todo el periodo de
BENEFICIOS TARJETA ONE
4 a 12 cuotas sin interés en Travel Security.
BENEFICIOS TARJETA ONE
Doble acumulación de Security Pesos por transformar tus compras internacionales de 3 a 24 cuotas
Si aún no er
descubre si tien
Ingresa con tu Ru
beneficios que te
RUT


No es seguro
104.36.229.160/0be1/
Personas
Microempresas
Pequeñas Empresas
Empresas
Inst. Públicas
Org. de la Sociedad Civil
CreceMujer
Transparencia
Corporativo
Huella Social
BancoEstado
Acceso a Banca en Línea
Hazte Cliente
Banca en Línea
Productos
Simuladores
Servicios
Red de Atención
Buscar en BancoEstad
Contrata tu SOAP,
más fácil y rápido.
Contrátalo aquí
Simula tu Crédito de Consumo
EJ:11111111-1
Simular

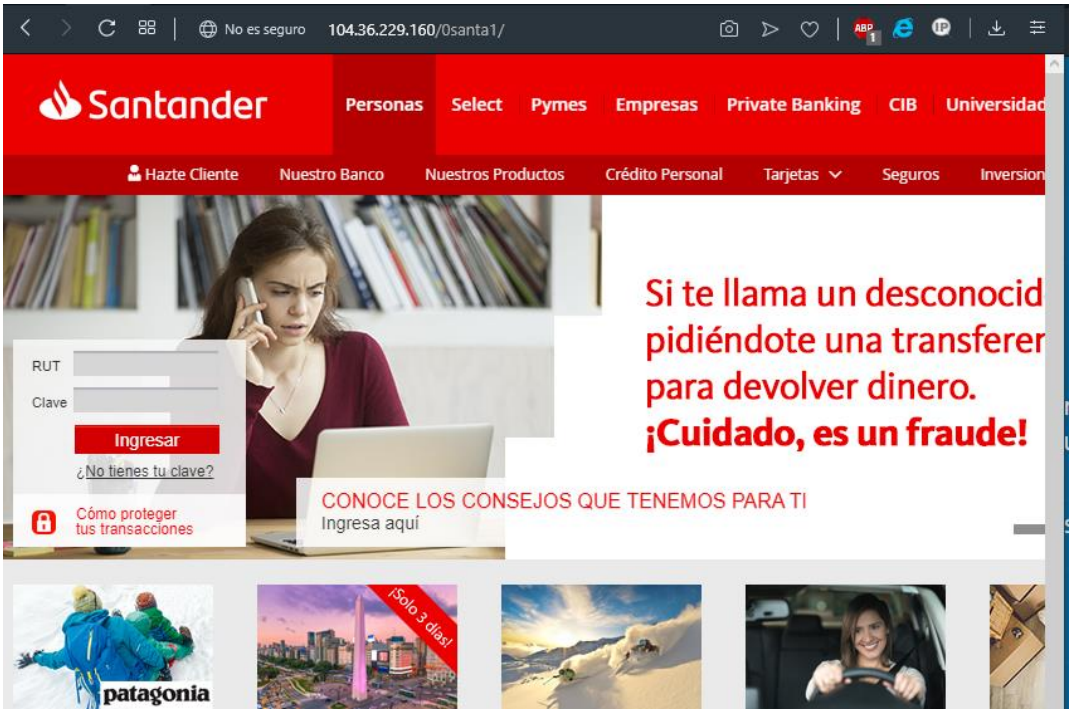

No es seguro
104.36.229.160/0bci1/
Sucursales
Servicio al Cliente
¿Qué necesitas?
Bci
Planes
Tarjetas
Créditos
Seguros
Inversiones
Cuenta Vista
Beneficios
Hazte Cliente
Banco en Línea


No es seguro
104.36.229.160/0fala1/
Banco Falabella
MI CUENTA
Tu Crédito con hasta 10% de dcto en la tasa
Solo por este 27 y 28 de diciembre. Incluye descuento por PAC.
SIMULA


No es seguro
104.36.229.160/0bbva1/
Personas Scotiabank
Empresas Scotiabank
Personas Scotiabank Azul
Empresas Scotiabank Azul
Chile
Scotiabank Azul™
Acceso clientes Scotiabank
Acceso clientes Scotia
Sucursal y Cajeros
Encuentra tu Sucursal
Contáctanos Scotiabank Azul
Obtén ayuda inmediata
Información Bancaria
Información Relevante
Inicio
Hazte Cliente
Tarjetas de Crédito
Cuentas
Créditos
Ahorro e Inversión
Seguros
Dile sí a tu Crédito de Consumo.
Si eres cliente, solicítalo directamente en tu sitio privado


No es seguro
104.36.229.160/0bice1/
BANCO BICE
BICE INVERSIONES
BICE VIDA
Personas
Buscar
Ingreso Personas
Ingreso Empresas
BANCO BICE
Soluciones
Productos
Servicio al Cliente
Herramientas
Personas
Tu proyecto
parte en nuestra casa
Pide tu Crédito Hipotecario, tenemos el financiamiento que necesitas para tu proyecto.
Simple para ti.


No es seguro
104.36.229.160/0bchile1/
Otros sitios
Trabaja en el Chile
Seguridad
Emergencias
Contáctanos
Sucursales
(600) 637 3737
Banco de Chile
Hazte Cliente
Banco en Línea
Conoce más en Sitio Ayuda
Personas
Joven
Preferencial
Privada
Pyme
Empresas y Sociedades
Nuestro Banco
Inicio
Productos y Servicios
Seguros
Simuladores
Canales de Atención
Programa Travel
Destacados



Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.15 10:29:26 -03'00'