Alerta de seguridad informática	**8FFR-00090-001**
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 las entidades bancarias aludidas.

Indicadores de Compromisos

URL´s

URL Sitio Clonado:
http[://]192[.]210[.]179[.]48/0bbva1/
http[://]192[.]210[.]179[.]48/0bice1/
http[://]192[.]210[.]179[.]48/0bchile1/
http[://]192[.]210[.]179[.]48/0ita1/
http[://]192[.]210[.]179[.]48/0santa1/
http[://]192[.]210[.]179[.]48/0rip1/
http[://]192[.]210[.]179[.]48/0office1/
http[://]192[.]210[.]179[.]48/0bs1/
http[://]192[.]210[.]179[.]48/0be1/
http[://]192[.]210[.]179[.]48/0bci1/
http[://]192[.]210[.]179[.]48/0fala1//

IP´s

192[.]210[.]179[.]48

IP address << 192.210.179.48 >>	
Block start	192.210.179.0
End of block	192.210.179.255
Block size	256 Domains in block
Block name	CC-192-210-179-0-24
AS number	36352
Parent block	192.210.128.0 - 192.210.255.255
Organization	Hudson Valley Host
City	Buffalo
Region/State	New York
Country	US , United States
Reg. date	2015-12-23
Host name	192-210-179-48-host.colocrossing.com
Domains	not found

Ilustración 1 Dirección Ip de Sitio Fraudulento a la Banca Chilena

Localización

Massachusetts, Estados Unidos

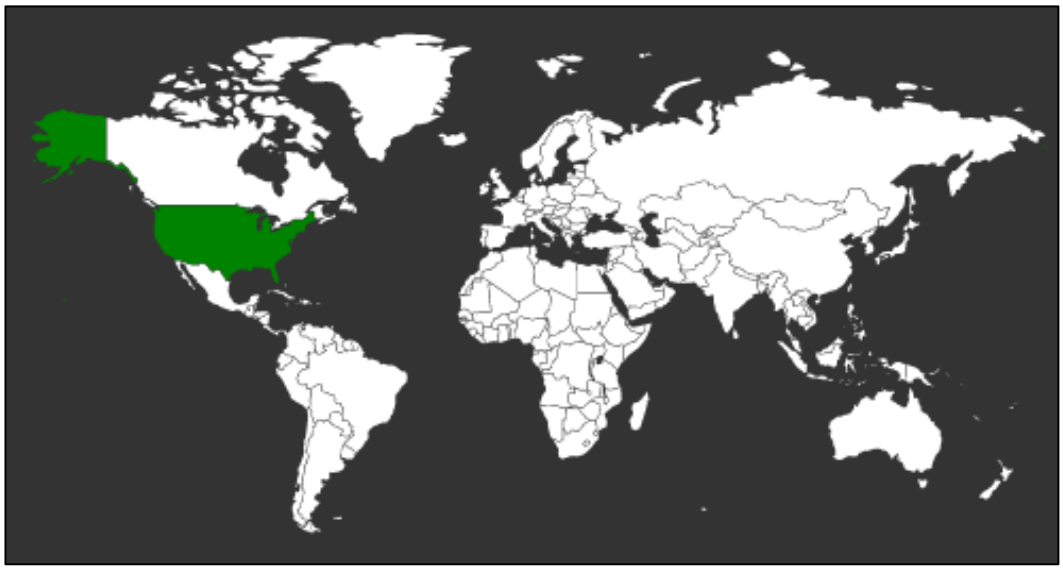
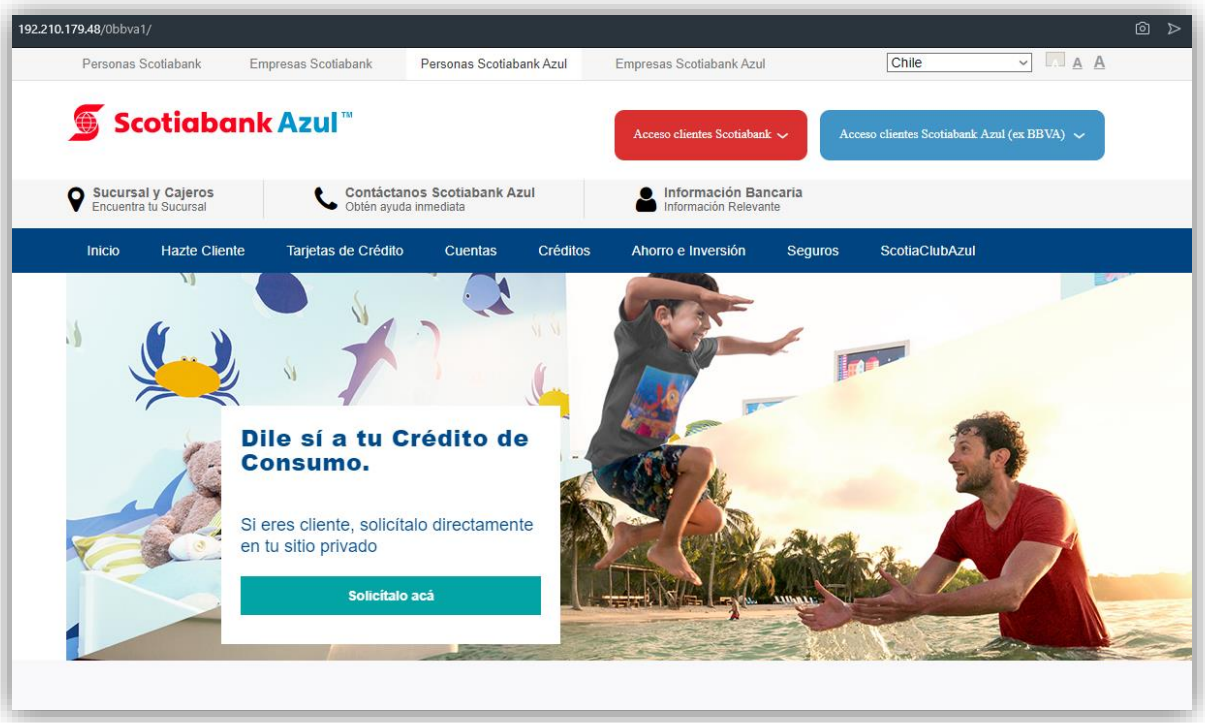
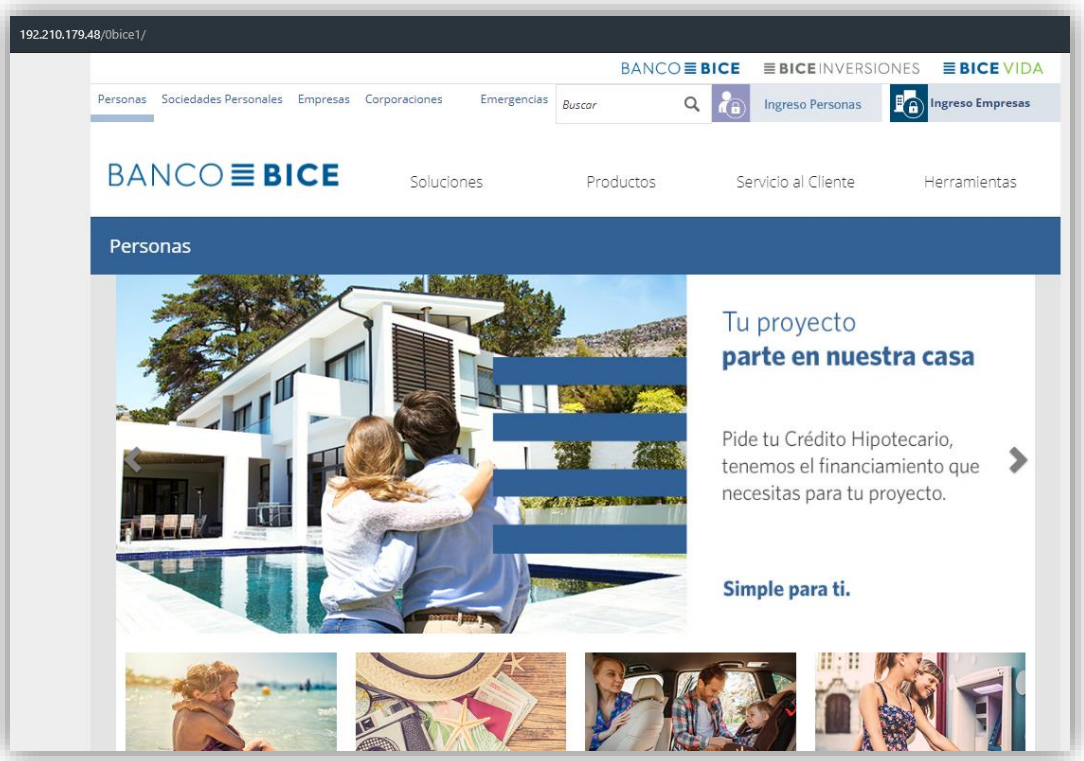
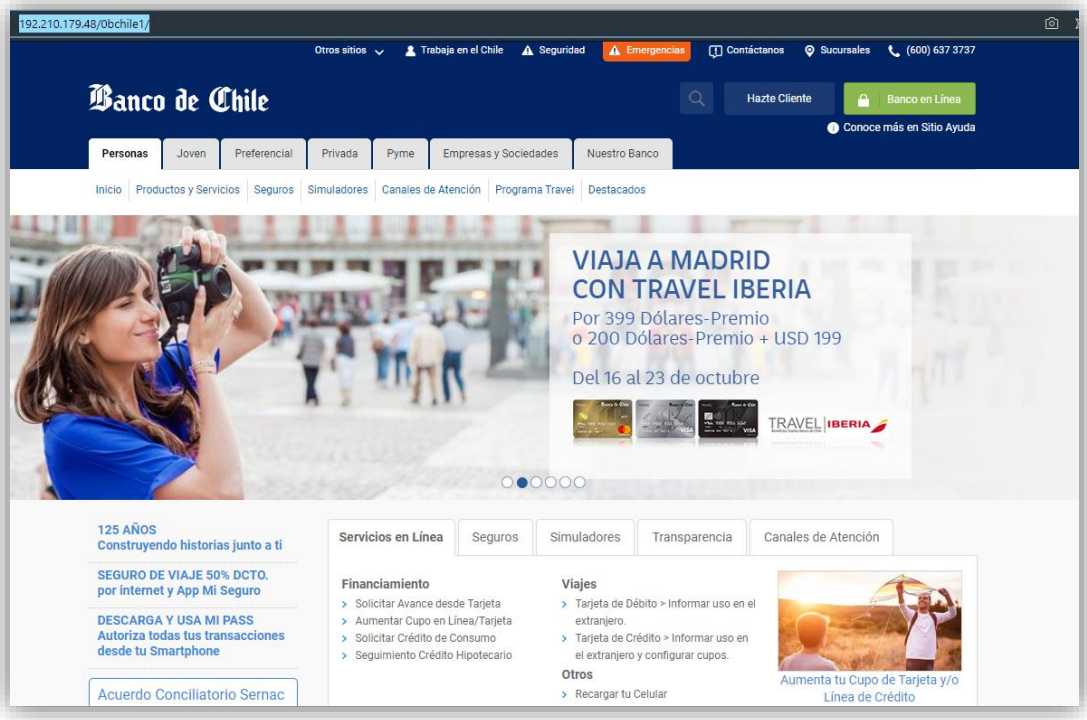
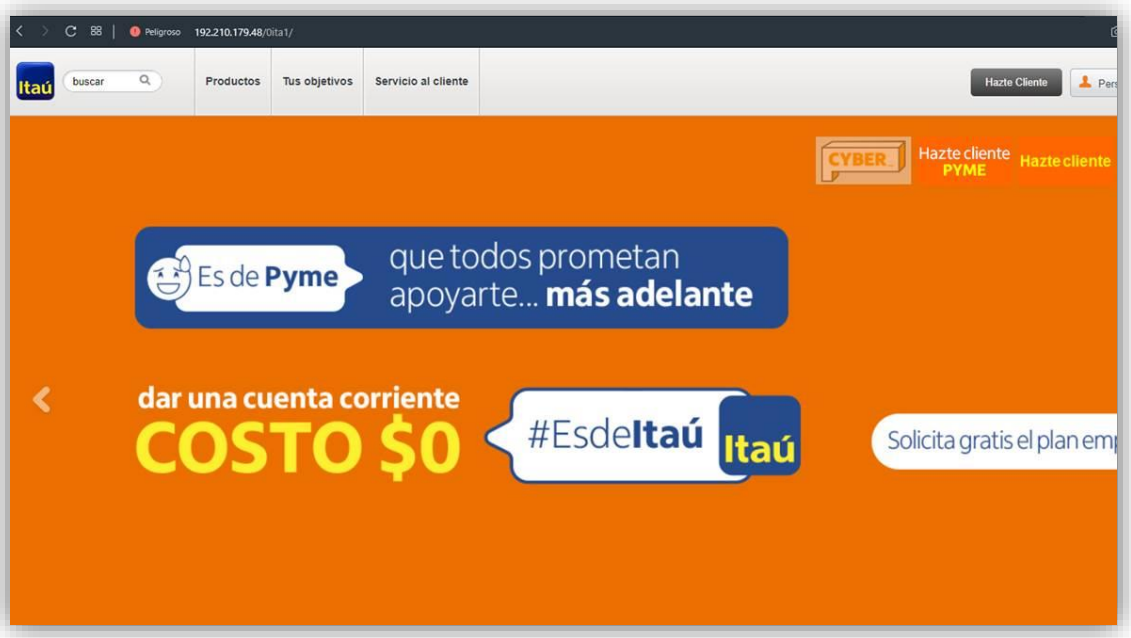


Imagen de los Sitios

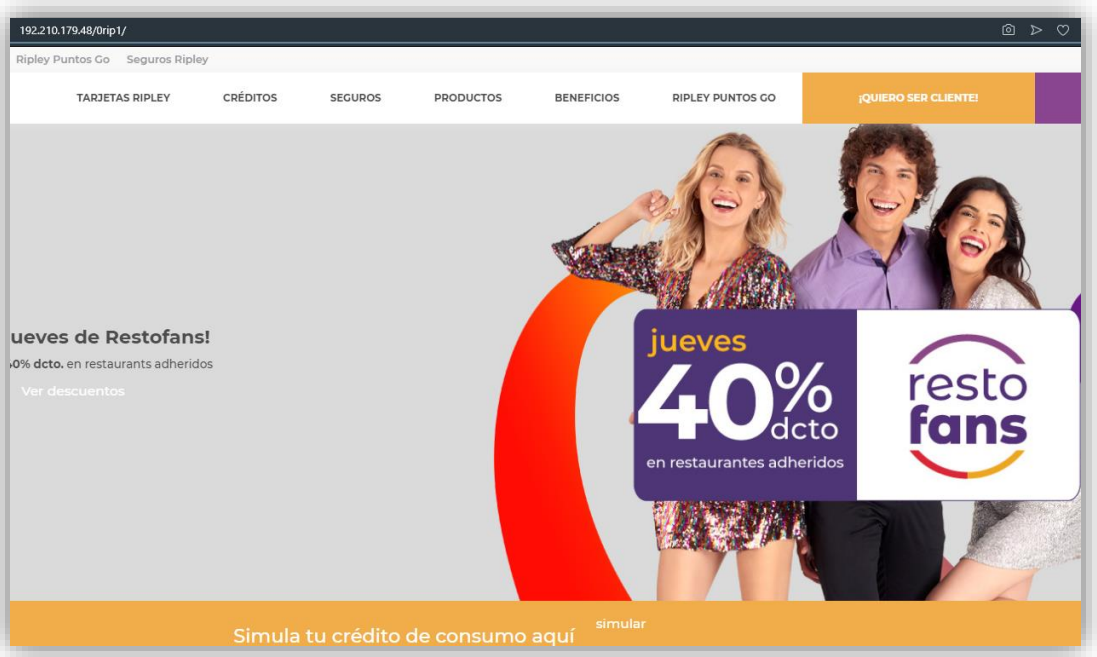


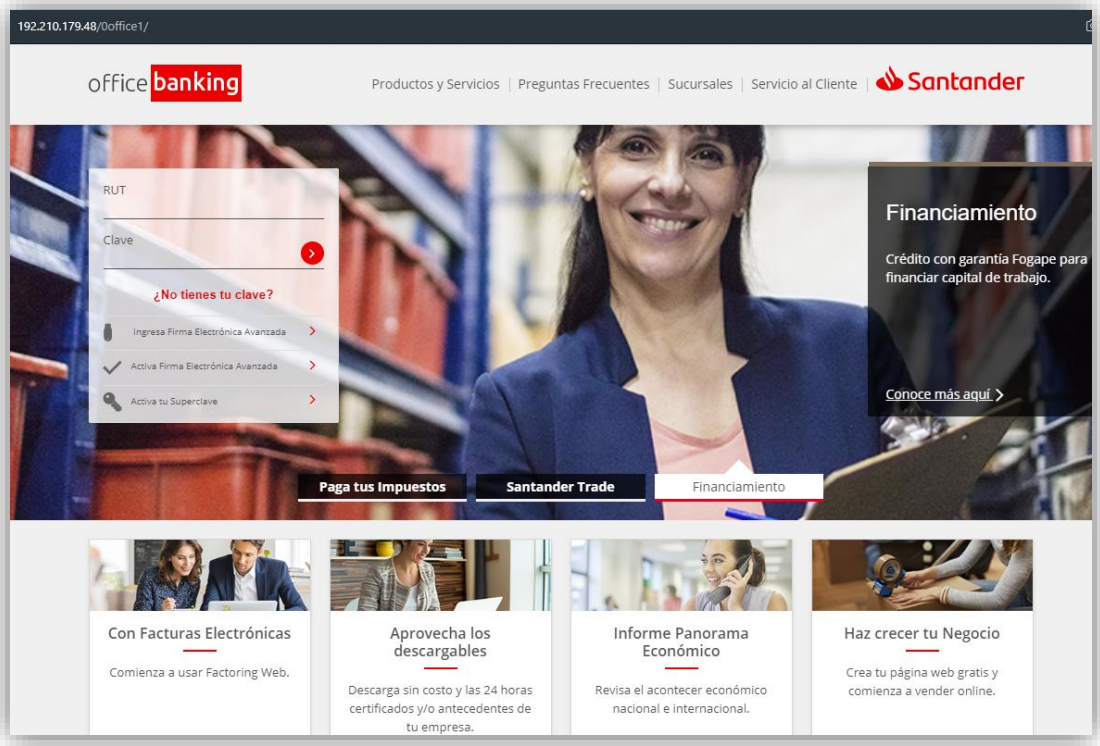

192.210.179.48/0bice1/
BANCO BICE
BICE INVERSIONES
BICE VIDA
Personas
Sociedades Personales
Empresas
Corporaciones
Emergencias
Buscar
Ingreso Personas
Ingreso Empresas
BANCO BICE
Soluciones
Productos
Servicio al Cliente
Herramientas
Personas
Tu proyecto
parte en nuestra casa
Pide tu Crédito Hipotecario, tenemos el financiamiento que necesitas para tu proyecto.
Simple para ti.

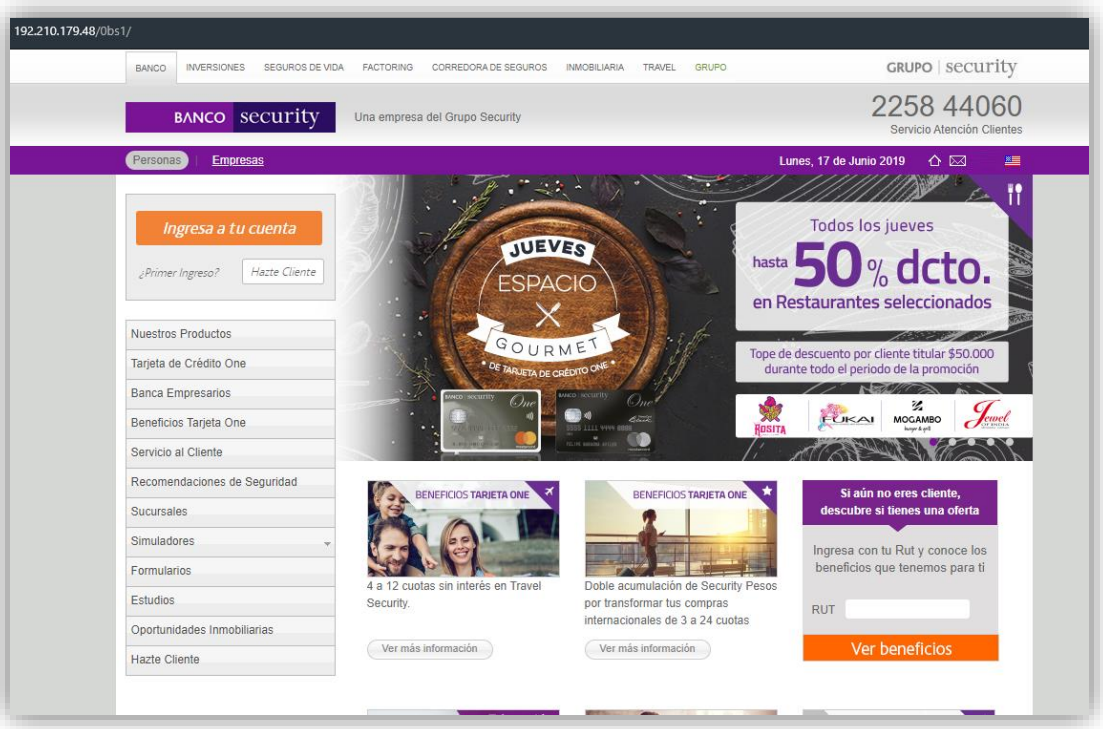

192.210.179.48/0bchile1/
Otros sitios
Trabaja en el Chile
Seguridad
Emergencias
Contáctanos
Sucursales
(600) 637 3737
Banco de Chile
Hazte Cliente
Banco en Línea
Conoce más en Sitio Ayuda
Personas
Joven
Preferencial
Privada
Pyme
Empresas y Sociedades
Nuestro Banco
Inicio
Productos y Servicios
Seguros
Simuladores
Canales de Atención
Programa Travel
Destacados
VIAJA A MADRID
CON TRAVEL IBERIA
Por 399 Dólares-Premio
o 200 Dólares-Premio + USD 199
Del 16 al 23 de octubre
TRAVEL IBERIA
125 AÑOS
Construyendo historias junto a ti
SEGURO DE VIAJE 50% DCTO.
por internet y App Mi Seguro
DESCARGA Y USA MI PASS
Autoriza todas tus transacciones desde tu Smartphone
Acuerdo Conciliatorio Sernac
Servicios en Línea
Seguros
Simuladores
Transparencia
Canales de Atención
Financiamiento
Solicitar Avance desde Tarjeta
Aumentar Cupo en Línea/Tarjeta
Solicitar Crédito de Consumo
Seguimiento Crédito Hipotecario
Viajes
Tarjeta de Débito > Informar uso en el extranjero.
Tarjeta de Crédito > Informar uso en el extranjero y configurar cupos.
Otros
Recargar tu Celular
Aumenta tu Cupo de Tarjeta y/o Línea de Crédito

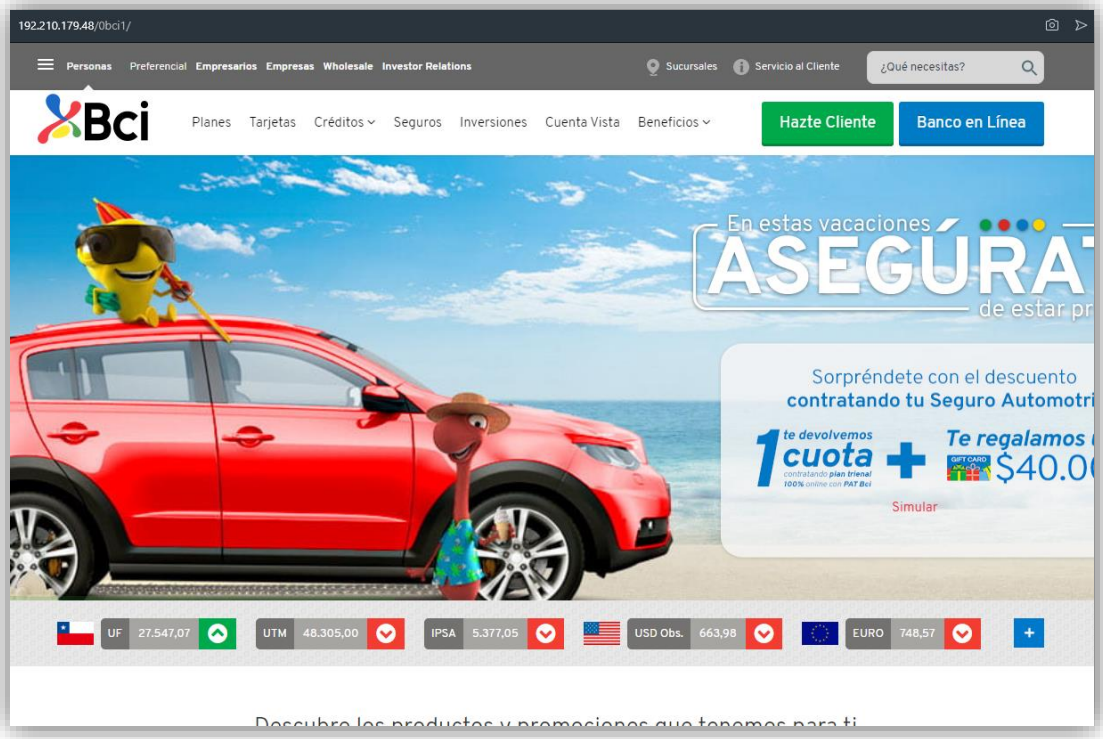

Peligroso 192.210.179.48/0ita1/
Itaú
buscar
Productos
Tus objetivos
Servicio al cliente
Hazte Cliente
CYBER
Hazte cliente PYME
Hazte cliente
Es de Pyme
que todos prometan apoyarte... más adelante
dar una cuenta corriente
COSTO $0
#EsdeItaú
Itaú
Solicita gratis el plan em


192.210.179.48/0santa1/
Santander
Personas
Select
Pymes
Empresas
Private Banking
CIB
Universidades
Beneficios
Hazte Cliente
Nuestro Banco
Nuestros Productos
Crédito Personal
Tarjetas
Seguros
Inversiones
Mundo Hipotecario
RUT
Clave
Ingresar
¿No tienes tu clave?
Cómo proteger tus transacciones
Si te llama un desconocido pidiéndote una transferencia para devolver dinero.
¡Cuidado, es un fraude!
CONOCE LOS CONSEJOS QUE TENEMOS PARA TI
Ingresa aquí
Servicio al Cliente
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 tu Crédito Personal
Si eres cliente o no cliente, revisa si tienes un monto pre aprobado o Simula tu Crédito Personal aquí.
Reconocimientos
Sanodelucas.cl
SEGURO SALUD
SANTANDER LIFE
Santander presenta Life.
Por primera vez un banco
Bienvenida


192.210.179.48/0rip1/
Ripley Puntos Go
Seguros Ripley
TARJETAS RIPLEY
CRÉDITOS
SEGUROS
PRODUCTOS
BENEFICIOS
RIPLEY PUNTOS GO
¡QUIERO SER CLIENTE!
ueves de Restofans!
0% dcto. en restaurants adheridos
Ver descuentos
jueves
40% dcto
en restaurantes adheridos
resto fans
Simula tu crédito de consumo aquí
simular


192.210.179.48/0office1/
office banking
Productos y Servicios
Preguntas Frecuentes
Sucursales
Servicio al Cliente
Santander
RUT
Clave
¿No tienes tu clave?
Ingresa Firma Electrónica Avanzada
Activa Firma Electrónica Avanzada
Activa tu Superclave
Financiamiento
Crédito con garantía Fogape para financiar capital de trabajo.
Conoce más aquí
Paga tus Impuestos
Santander Trade
Financiamiento
Con Facturas Electrónicas
Comienza a usar Factoring Web.
Aprovecha los descargables
Descarga sin costo y las 24 horas certificados y/o antecedentes de tu empresa.
Informe Panorama Económico
Revisa el acontecer económico nacional e internacional.
Haz crecer tu Negocio
Crea tu página web gratis y comienza a vender online.


192.210.179.48/0bs1/
BANCO
INVERSIONES
SEGUROS DE VIDA
FACTORING
CORREDORA DE SEGUROS
INMOBILIARIA
TRAVEL
GRUPO
GRUPO | security
BANCO security
Una empresa del Grupo Security
2258 44060
Servicio Atención Clientes
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
Hazte Cliente
JUEVES
ESPACIO
GOURMET
DE TARJETA DE CRÉDITO ONE
Todos los jueves
hasta 50% dcto.
en Restaurantes seleccionados
Tope de descuento por cliente titular $50.000
durante todo el periodo de la promoción
ROSITA
FUKAI
MOGAMBO
Jewel
BENEFICIOS TARJETA ONE
4 a 12 cuotas sin interés en Travel Security.
Ver más información
BENEFICIOS TARJETA ONE
Doble acumulación de Security Pesos por transformar tus compras internacionales de 3 a 24 cuotas
Ver más información
Si aún no eres cliente, descubre si tienes una oferta
Ingresa con tu Rut y conoce los beneficios que tenemos para ti
RUT
Ver beneficios


192.210.179.48/0bci1/
Personas
Preferencial
Empresarios
Empresas
Wholesale
Investor Relations
Sucursales
Servicio al Cliente
¿Qué necesitas?
Bci
Planes
Tarjetas
Créditos
Seguros
Inversiones
Cuenta Vista
Beneficios
Hazte Cliente
Banco en Línea
En estas vacaciones
ASEGÚRA
de estar pr
Sorpréndete con el descuento
contratando tu Seguro Automotri
1 cuota
Te regalamos
$40.0
Simular
UF 27.547,07
UTM 48.305,00
IPSA 5.377,05
USD Obs. 663,98
EURO 748,57
Descubre los productos y promociones que tenemos para ti


192.210.179.48/0fala1/
Sodimac Tottus Homy Linio
Banco Falabella
MI CUENTA
CUENTAS | CRÉDITOS | TARJETAS DE CRÉDITOS | AHORRO E INVERSIONES | SEGUROS | CMR PUNTOS | BENEFICIOS | AYUDA Y CONTACTO
Tu Crédito con hasta 10% de dcto en la tasa
Solo por este 27 y 28 de diciembre. Incluye descuento por PAC.
SIMULA
tu CRÉDITO DE CONSUMO
RUT
SIMULAR


192.210.179.48/0be1/
Personas Microempresas Pequeñas Empresas Empresas Inst. Públicas Org. de la Sociedad Civil CreceMujer Transparencia Corporativo Huella Social
BancoEstado
Hazte Cliente
Banca en Línea
Productos Simuladores Servicios Red de Atención
Buscar en BancoEstado...
Paga con tus Tarjetas de Crédito de 4 a 12 cuotas sin interés.
Paga con tus
Tarjetas de Crédito de:
4 a 12 cuotas sin interés
Infórmate aquí
Simula tu Crédito de Consumo
EJ:11111111-1
Simular

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 09:25:54 -03'00'