

Alerta de seguridad informática	8FFR20-00199-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Enero de 2020
Última revisión	30 de Enero 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 afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC 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 11 portales fraudulentos asociado a una IP que suplantan diferentes sitios web oficiales de los bancos Estado, Security, de Chile, BCI, Scotiabank, Falabella, Santander, BICE, ITAU y Ripley. Estos portales podrían servir para robar credenciales de usuarios de esas entidades.

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

107[.]191[.]126[.]175/Ofala1/
 107[.]191[.]126[.]175/Osanta1/
 107[.]191[.]126[.]175/Ooffice1/
 107[.]191[.]126[.]175/Orip1/
 107[.]191[.]126[.]175/Oita1/
 107[.]191[.]126[.]175/Obice1/
 107[.]191[.]126[.]175/Obci1/
 107[.]191[.]126[.]175/Obchile1/
 107[.]191[.]126[.]175/Obbva1/
 107[.]191[.]126[.]175/Obs1/
 107[.]191[.]126[.]175/Obe1/

Ilustración 1 Dominio donde se Aloja Url del Banca Nacional, Falso y DNS que utiliza

IP

107.191.126.175



IP address << 107.191.126.175 >>	
Block start	107.191.96.0
End of block	107.191.127.255
Block size	8192  Domains in block
Block name	RAMNODE-9
AS number	3842
Parent block	107.0.0.0 - 107.255.255.255
Organization	RamNode LLC
City	Smarr
Region/State	Georgia
Country	 US , United States
Reg. date	2014-05-08
Host name	no record in reverse zone
Domains	not found

Ilustración 2 Ip de Origen donde se aloja Sitio Falso del Banca Nacional.

Localización

Atlanta, Georgia, Estados Unidos

Location	Atlanta, Georgia, United States (US) 
Latitude and Longitude	33.83, -84.38



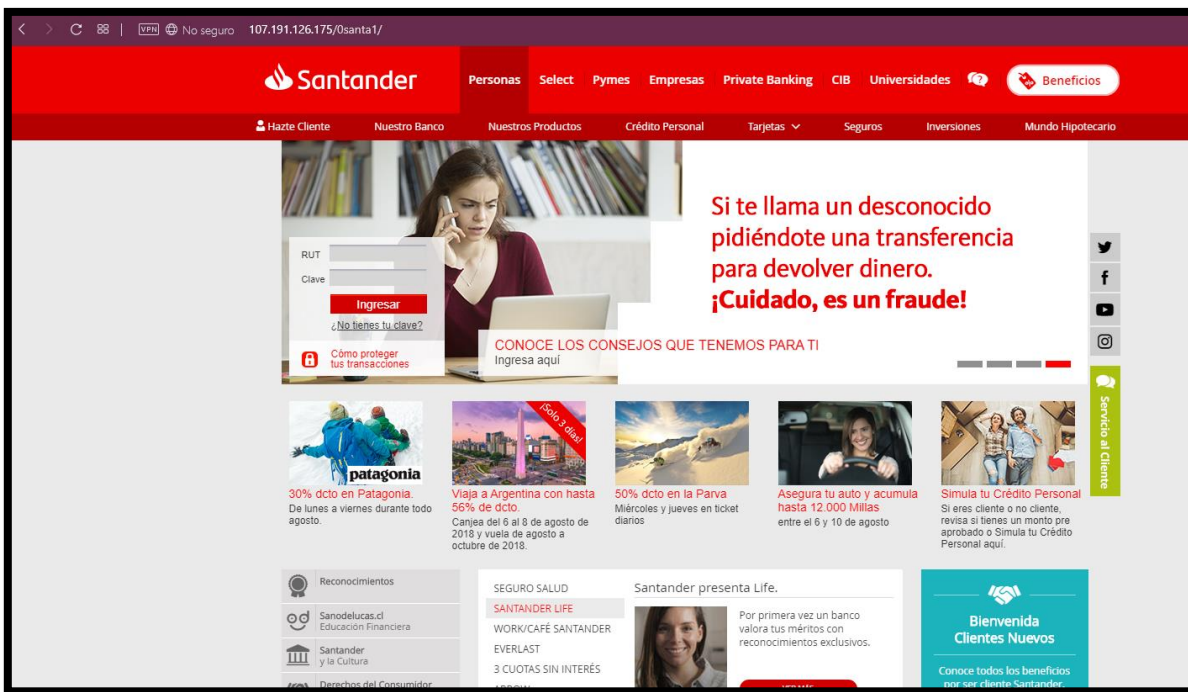
Imagen del sitio

107[.]191[.]126[.]175/Ofala1/



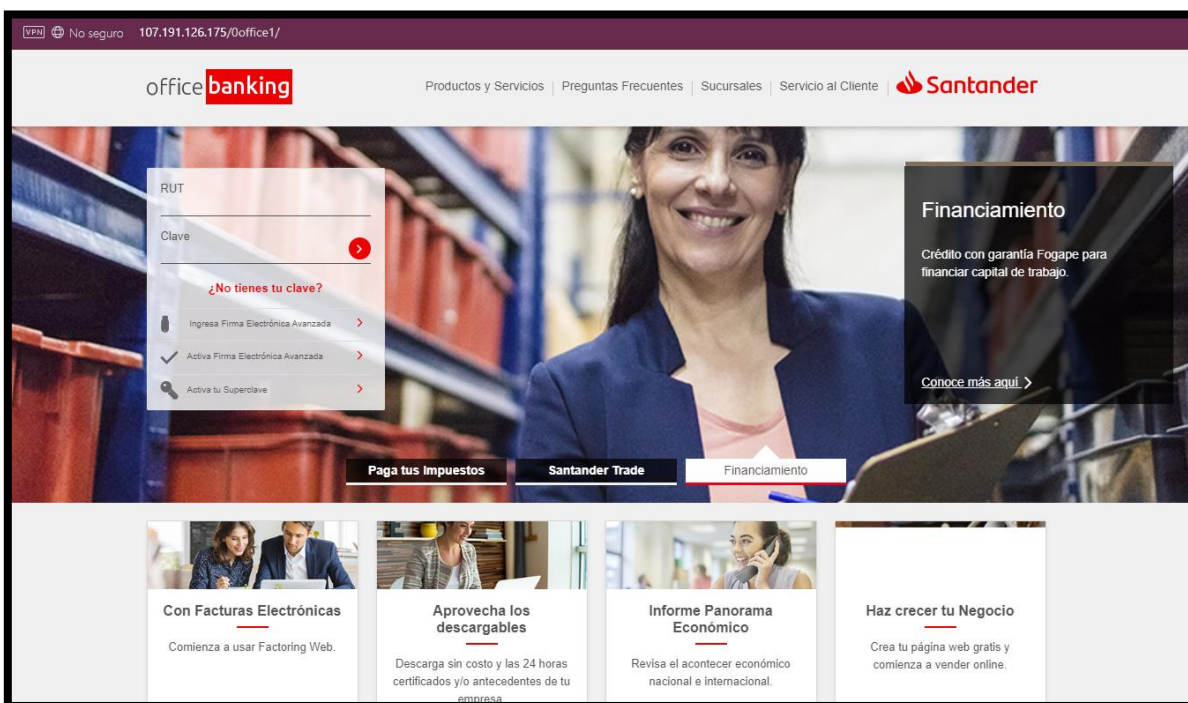
A screenshot of the Banco Falabella website. The browser address bar shows '107.191.126.175/Ofala1/'. The website header includes the Banco Falabella logo and a navigation menu with items: CUENTAS | CRÉDITOS | TARJETAS DE CRÉDITOS | AHORRO E INVERSIONES | SEGUROS | CMR PUNTOS | BENEFICIOS | AYUDA Y CONTACTO. A 'MI CUENTA' button is visible in the top right. The main content area features a large image of a smiling couple in a hammock. Overlaid on the image is a circular graphic with the text: 'Tu Crédito con hasta 10% de dcto en la tasa'. Below this, smaller text reads: 'Solo por este 27 y 28 de diciembre. Incluye descuento por PAC.' A red 'SIMULA' button is positioned below the text. At the bottom of the page, there is a form to 'Simula tu CRÉDITO DE CONSUMO' with a 'RUT' input field and a green 'SIMULAR' button.

107[.]191[.]126[.]175/Osanta1/



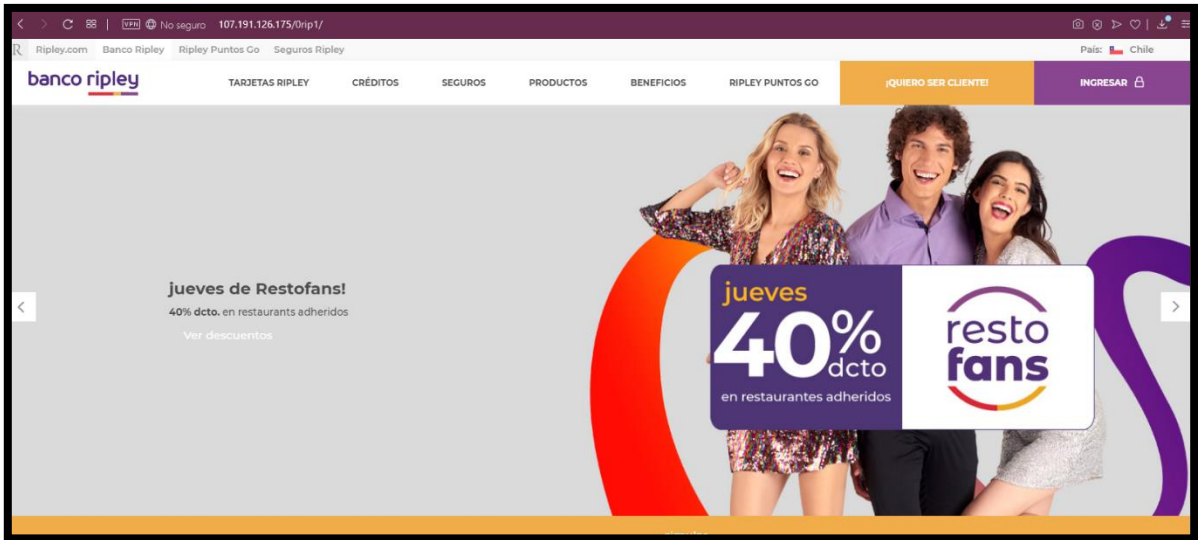
The screenshot shows the Santander Chile website. The top navigation bar includes links for Personas, Select, Pymes, Empresas, Private Banking, CIB, Universidades, and Beneficios. Below this is a secondary navigation bar with links like Hazte Cliente, Nuestro Banco, Nuestros Productos, Crédito Personal, Tarjetas, Seguros, Inversiones, and Mundo Hipotecario. The main content area features a large banner with a woman on a phone and a laptop, with the text: "Si te llama un desconocido pidiéndote una transferencia para devolver dinero. ¡Cuidado, es un fraude!". Below the banner are several promotional tiles: "patagonia" (30% dcto en Patagonia), "Viaja a Argentina con hasta 56% de dcto", "50% dcto en la Parva", "Asegura tu auto y acumula hasta 12.000 Millas", and "Simula tu Crédito Personal". There are also sections for "Reconocimientos", "SEGURO SALUD", "Santander presenta Life", and "Bienvenida Clientes Nuevos".

107[.]191[.]126[.]175/Office1/

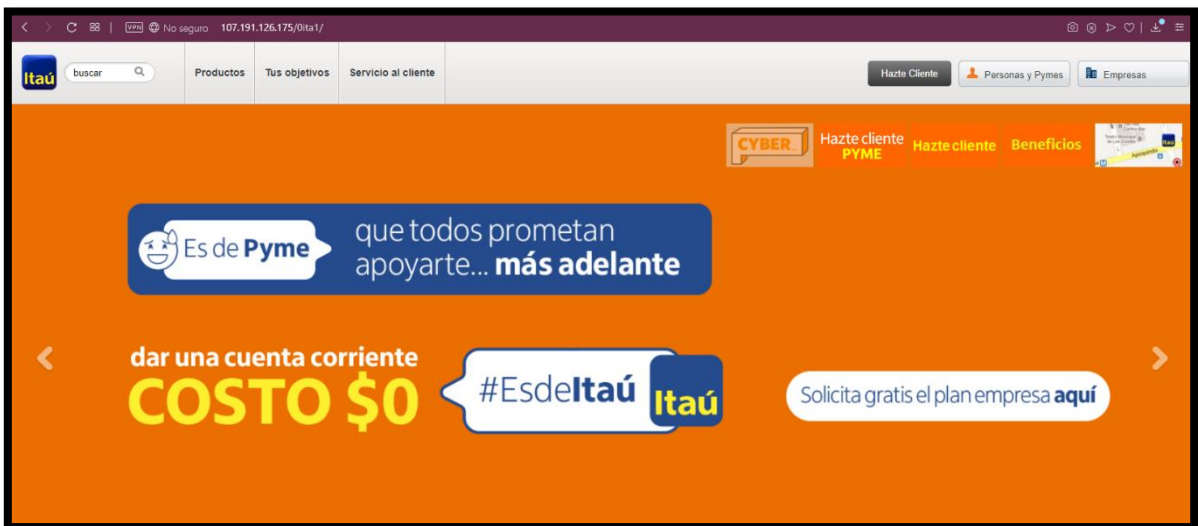


The screenshot shows the Santander Office Banking website. The top navigation bar includes links for Productos y Servicios, Preguntas Frecuentes, Sucursales, Servicio al Cliente, and the Santander logo. The main content area features a large banner with a smiling woman, with the text: "Financiamiento. Crédito con garantía Fogape para financiar capital de trabajo. Conoce más aquí". Below the banner are several promotional tiles: "Paga tus Impuestos", "Santander Trade", "Financiamiento", "Con Facturas Electrónicas", "Aprovecha los descargables", "Informe Panorama Económico", and "Haz crecer tu Negocio".

107[.]191[.]126[.]175/Orip1/



107[.]191[.]126[.]175/Oita1/



107[.]191[.]126[.]175/Obice1/



107.191.126.175/Obice1/

BANCO **BICE** **BICE INVERSIONES** **BICE VIDA**

Personas Sociedades Personales Empresas Corporaciones Emergencias Ingreso Personas Ingreso Empresas

BANCO BICE Soluciones Productos Servicio al Cliente Herramientas

Personas

3 a 12 Cuotas sin Interés en Educación

Beneficio exclusivo de tus Tarjetas de Crédito Visa Banco BICE. ➔

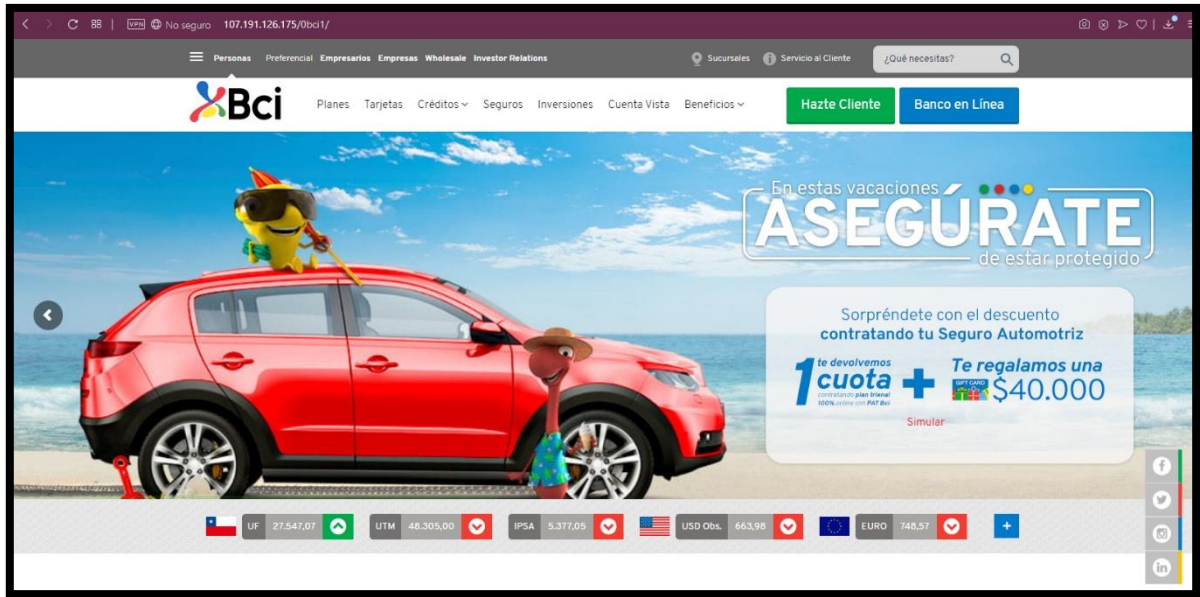
Simple para ti.

Compra, transfiere o retira Dólares y Euros en tu banco en línea

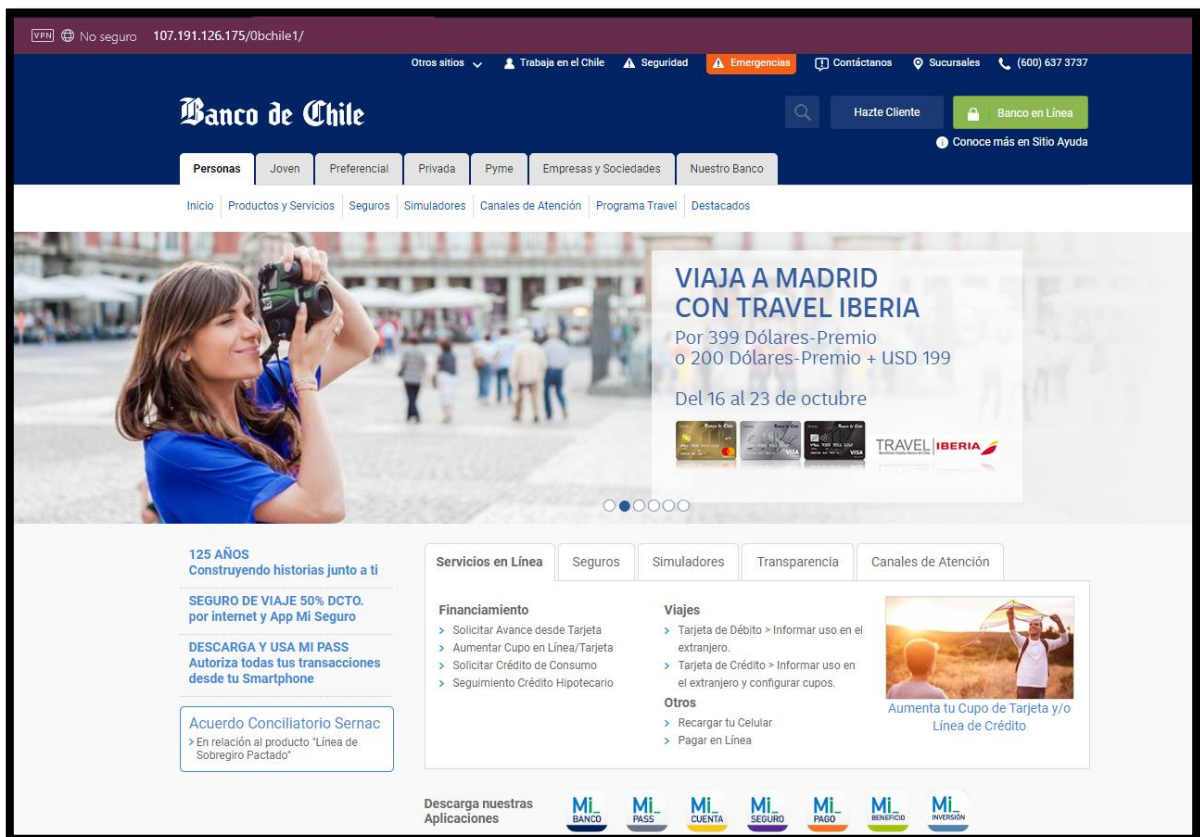
Protege tu auto con BICE Corredores de Seguros

Retira hasta \$400.000 diarios

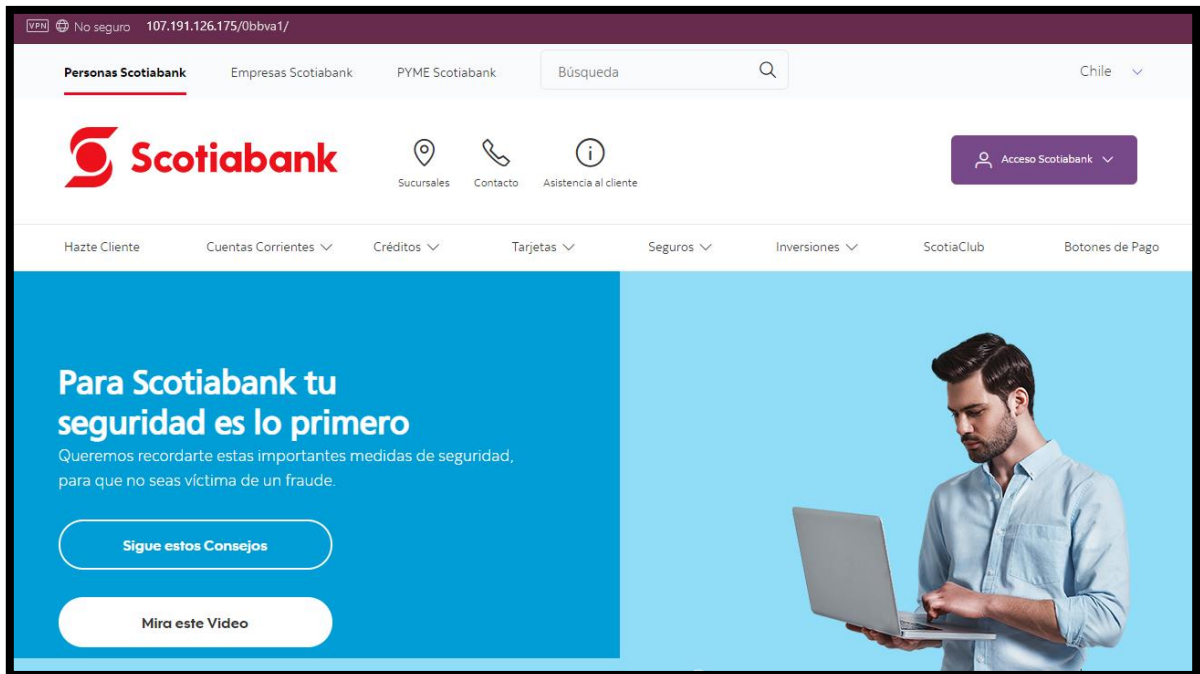
107[.]191[.]126[.]175/Obci1/



107[.]191[.]126[.]175/Obchile1/



107.[.]191[.]126[.]175/Obbva1/



107.191.126.175/Obbva1/

VPNI No seguro 107.191.126.175/Obbva1/

Personas Scotiabank Empresas Scotiabank PYME Scotiabank Búsqueda Chile

Scotiabank Sucursales Contacto Asistencia al cliente Acceso Scotiabank

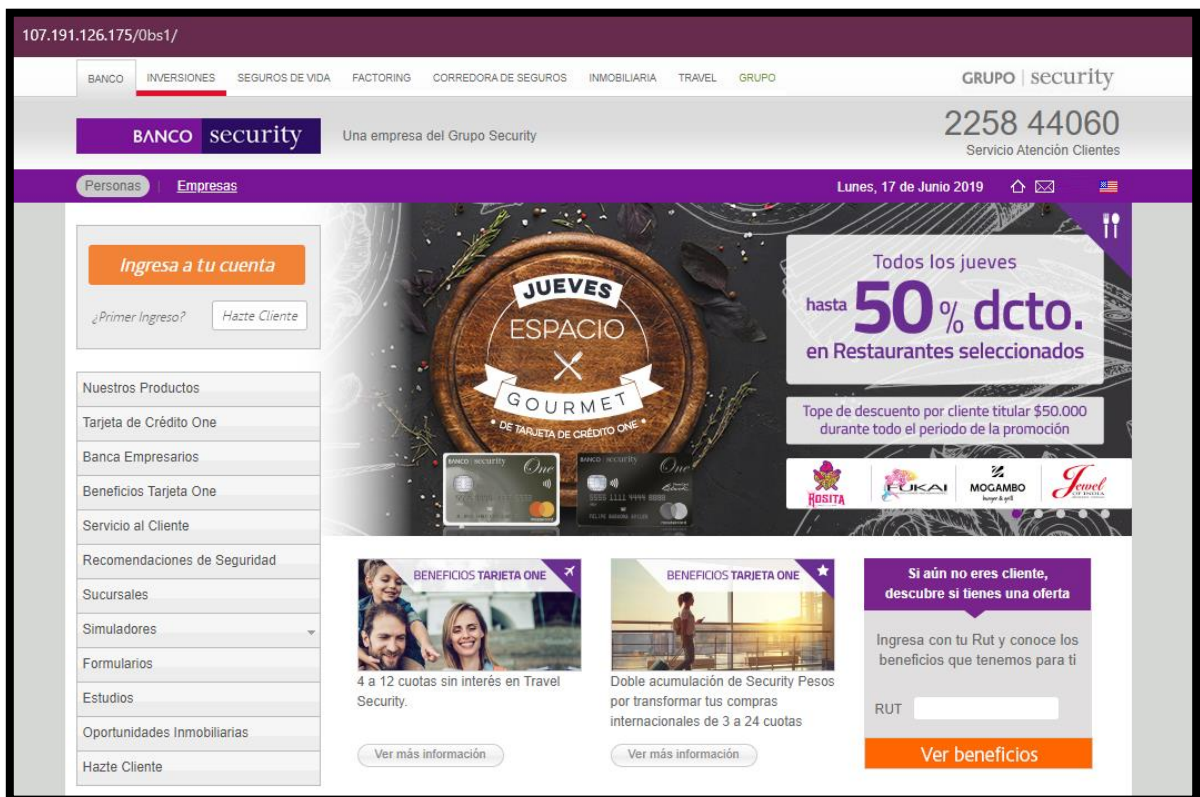
Hazte Cliente Cuentas Corrientes Créditos Tarjetas Seguros Inversiones ScotiaClub Botones de Pago

Para Scotiabank tu seguridad es lo primero
Queremos recordarte estas importantes medidas de seguridad, para que no seas víctima de un fraude.

Sigue estos Consejos

Mira este Video

107.[.]191[.]126[.]175/Obs1/



107.191.126.175/Obs1/

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

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

HOSTIA FUKAI MOGAMBO Jewel

BENEFICIOS TARIETA ONE
4 a 12 cuotas sin interés en Travel Security.

BENEFICIOS TARIETA ONE
Doble acumulación de Security Pesos por transformar tus compras internacionales de 3 a 24 cuotas

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

107[.]191[.]126[.]175/0be1/



The screenshot shows a fraudulent website designed to look like the official BancoEstado website. The URL in the address bar is 107.191.126.175/0be1/. The page features the BancoEstado logo, navigation menus for various services, and a prominent advertisement for credit cards. The ad text reads: 'Paga con tus Tarjetas de Crédito de: 4 a 12 cuotas sin interés'. Below this, there are images of Visa and Mastercard credit cards and a red button that says 'Infórmate aquí'. At the bottom of the ad, there is a form labeled 'Simula tu Crédito de Consumo' with an input field containing 'Ej:11111111-1' and a 'Simular' button. The text 'Beneficios del mes' is partially visible at the bottom of the page.

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.