

Alerta de seguridad informática	8FFR-00031-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Agosto de 2019
Última revisión	29 de Agosto de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial del **bancoestado.cl**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

<http://estado-personas.online/login/comun2019/banca-en-linea-personas.html>

IP's

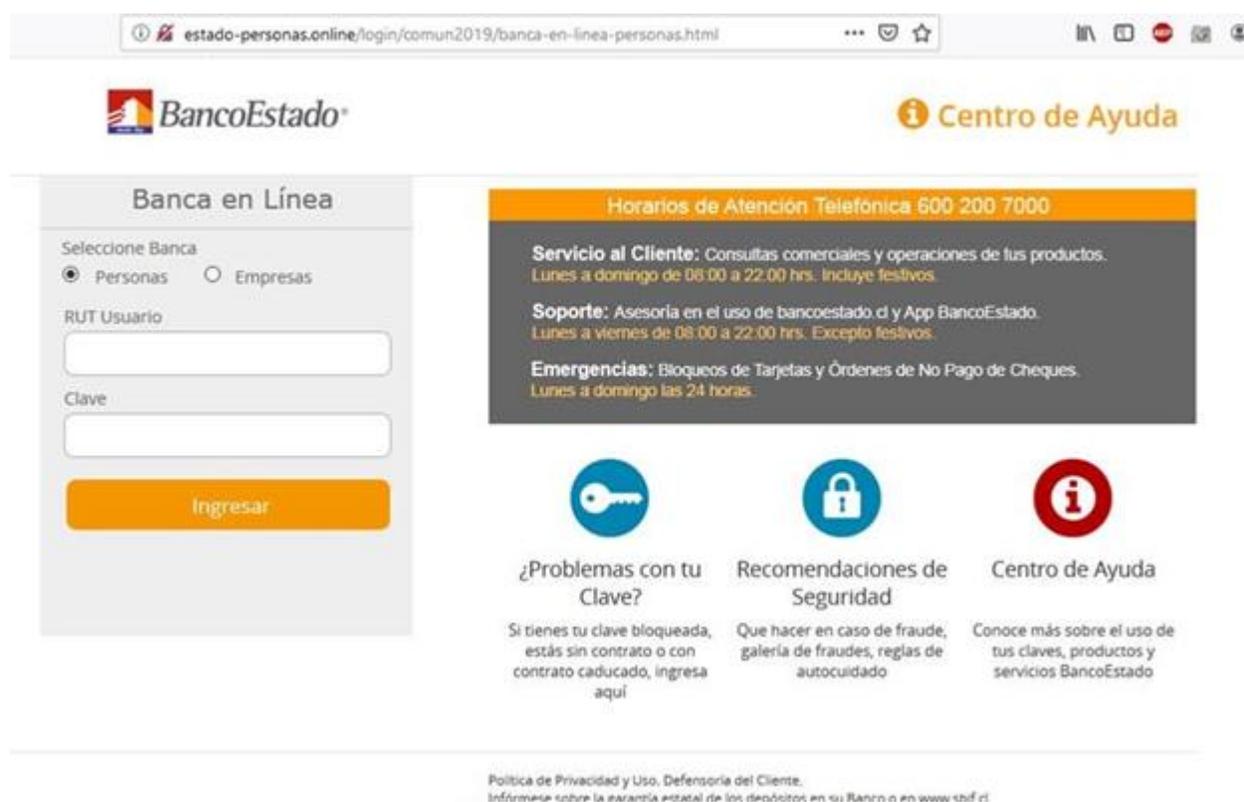
192.254.185.30

Localización

United States

Provo, Utah

Ejemplo de Imagen del sitio



The screenshot shows the BancoEstado online banking login page. The browser address bar displays the URL: estado-personas.online/login/comun2019/banca-en-linea-personas.html. The page features the BancoEstado logo and a 'Centro de Ayuda' (Help Center) link. The main content area is divided into two sections. On the left, under 'Banca en Línea', there is a login form with radio buttons for 'Personas' (selected) and 'Empresas', a 'RUT Usuario' field, a 'Clave' field, and an 'Ingresar' button. On the right, there is a 'Horarios de Atención Telefónica 600 200 7000' section with three sub-sections: 'Servicio al Cliente' (consultas comerciales y operaciones de tus productos), 'Soporte' (asesoría en el uso de bancoestado.cl y App BancoEstado), and 'Emergencias' (bloqueos de Tarjetas y Órdenes de No Pago de Cheques). Below these are three icons representing '¿Problemas con tu Clave?', 'Recomendaciones de Seguridad', and 'Centro de Ayuda', each with a brief description of the service.

estado-personas.online/login/comun2019/banca-en-linea-personas.html

BancoEstado Centro de Ayuda

Banca en Línea

Seleccione Banca
 Personas Empresas

RUT Usuario

Clave

Ingresar

Horarios de Atención Telefónica 600 200 7000

Servicio al Cliente: Consultas comerciales y operaciones de tus productos.
Lunes a domingo de 08:00 a 22:00 hrs. Incluye festivos.

Soporte: Asesoría en el uso de bancoestado.cl y App BancoEstado.
Lunes a viernes de 08:00 a 22:00 hrs. Excepto festivos.

Emergencias: Bloqueos de Tarjetas y Órdenes de No Pago de Cheques.
Lunes a domingo las 24 horas.

¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí

Recomendaciones de Seguridad
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado

Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.stbf.cl

Whois

```
Domain Name: estado-personas.online
Registry Domain ID: D119840671-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-08-28T04:56:06Z
Creation Date: 2019-08-28T04:56:04Z
Registrar Registration Expiration Date: 2020-08-28T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: DISTRITO CAPITAL
Registrant Country: VE
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=estado-personas.online
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=estado-personas.online
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=estado-personas.online
Name Server: NS6321.HOSTGATOR.COM
Name Server: NS6322.HOSTGATOR.COM
DNSSEC: unsigned
```

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