

Alerta de seguridad cibernética	8FPH20-00253-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio 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 Smishing que supuestamente proviene de Banco Estado.

El atacante busca persuadir a la víctima para utilizar un enlace en el mensaje.

El mensaje informa que por motivos de seguridad se ha limitado sus operaciones en línea y solicita a la persona que use el enlace para verificar y activar la cuenta.

Al seleccionar el enlace, la persona es dirigida a un sitio falso de Banco Estado, 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:

hxxp://bit[.]ly/www-BancoEstado

http://192.119.71.107/

Urls sitio falso:

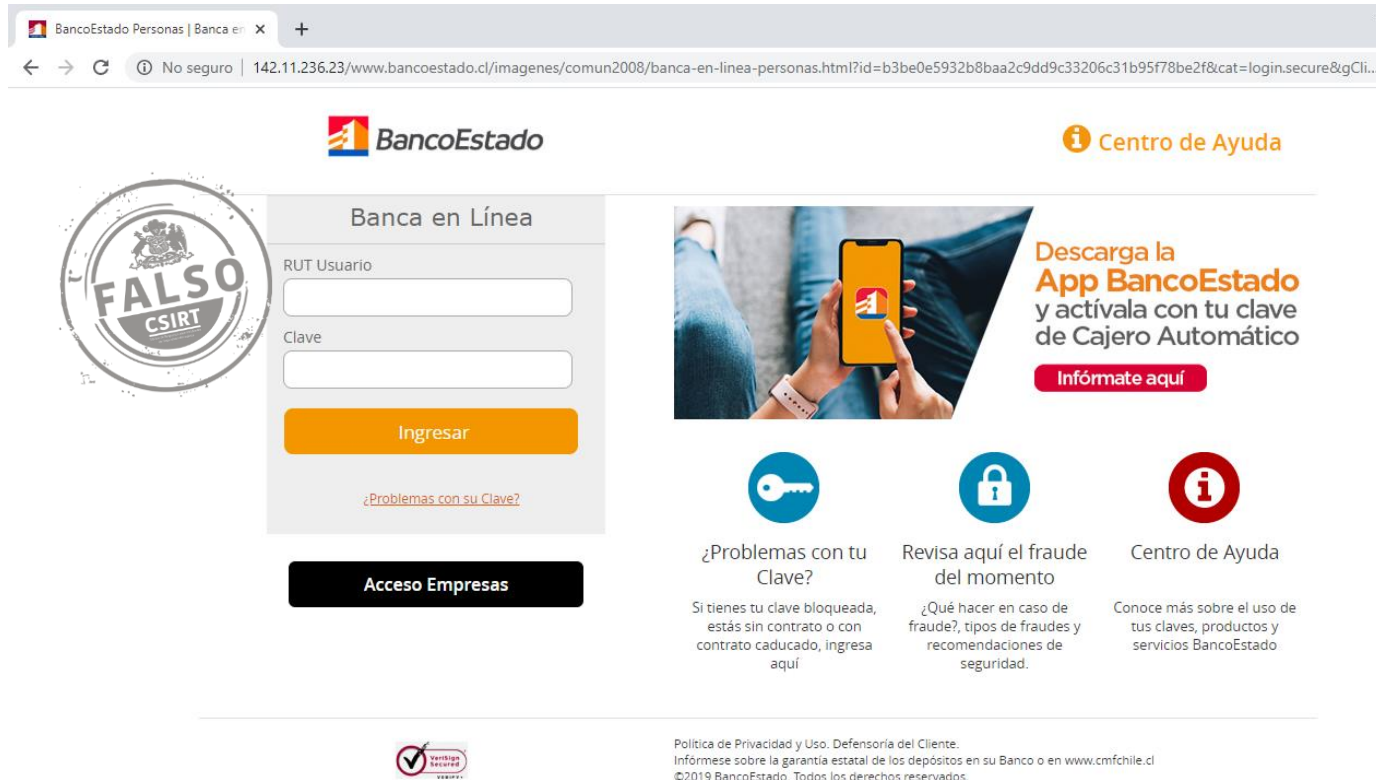
hxxp://142.11.236.23/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html

Imagen del mensaje

Banco Estado
Por motivos de seguridad
hemos limitado tus
operaciones en línea. Verifique
su cuenta para activar el
acceso: [https://bit.ly/www-
BancoEstado](https://bit.ly/www-BancoEstado)



Imagen del sitio



The screenshot shows the BancoEstado website's login page. At the top left, there is a browser tab for 'BancoEstado Personas | Banca en línea'. The address bar shows the URL: '142.11.236.23/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html?id=b3be0e5932b8baa2c9dd9c33206c31b95f78be2f&cat=login.secure&gCli...'. The page features the BancoEstado logo, a 'Centro de Ayuda' link, and a 'Banca en Línea' login form with fields for 'RUT Usuario' and 'Clave', and an 'Ingresar' button. A '¿Problemas con su Clave?' link is also present. To the right, there is a promotional banner for the 'App BancoEstado' with a 'Descarga la App BancoEstado y actívala con tu clave de Cajero Automático' message and an 'Infórmate aquí' button. Below the banner are three icons: a key for '¿Problemas con tu Clave?', a padlock for 'Revisa aquí el fraude del momento', and an information icon for 'Centro de Ayuda'. Each icon has a corresponding text block explaining the service. At the bottom, there is a 'Verificado' seal and a 'Política de Privacidad y Uso' link.

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.