

Alerta de seguridad cibernética	8FPH20-00222-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Mayo de 2020
Última revisión	16 de Mayo 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 phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del Banco Estado.

El mensaje del correo entrega falsa información sobre la entrega de un Bono de Emergencia Covid-19. A través de un enlace ubicado en el cuerpo del correo se invita a las personas a revisar si han recibido este beneficio entregado por el Instituto de Previsión Social y depositado en la cuenta RUT para evitar salir de tu casa.

Al seleccionar el enlace para revisar el supuesto depósito, la persona es dirigida a un sitio falso del banco donde se expone al robo de sus credenciales y de su tarjeta de coordenadas.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

**Urls Redirecciones:**

**Urls sitio falso:**

hxxp://consticaous[.]site/activala/imagenes/comun2008/banca-en-linea-personas.html

**Smtip Host**

[170.239.85.226]

**Sender**

apache@premiosourfs[.]com

**Asunto**

Beneficiario del Bono de Emergencia COVID-19!

## Imagen del mensaje



### Infórmate sobre el depósito del Bono de Emergencia COVID-19.

Beneficiarios y beneficiarias con el **Bono De Emergencia** Covid-19, pueden Visualizar [Aqui](#) .

Bienvenido(a), **Bono de Emergencia COVID-19**.

Es un bono especial que forma parte del Plan de Emergencia Económica del Gobierno, y que tiene como objetivo apoyar a las familias más vulnerables en la contingencia sanitaria por el COVID-19.

Dada la contingencia, el IPS ha instruido depositarlo en tu **CuentaRUT**, así no tendrás que salir de tu casa.

Visita [bonocovid.cl](#) o [www.bancoestado.cl](#) ingresa tu RUT en la consulta y conoce los detalles:

**Ingresar aquí**

**Ingresar en nuestra Banca en Línea** o [www.bonocovid.cl](#) y Veamos juntos Bono COVID-19 Chile: revisa si eres uno de los beneficiarios del subsidio del Gobierno

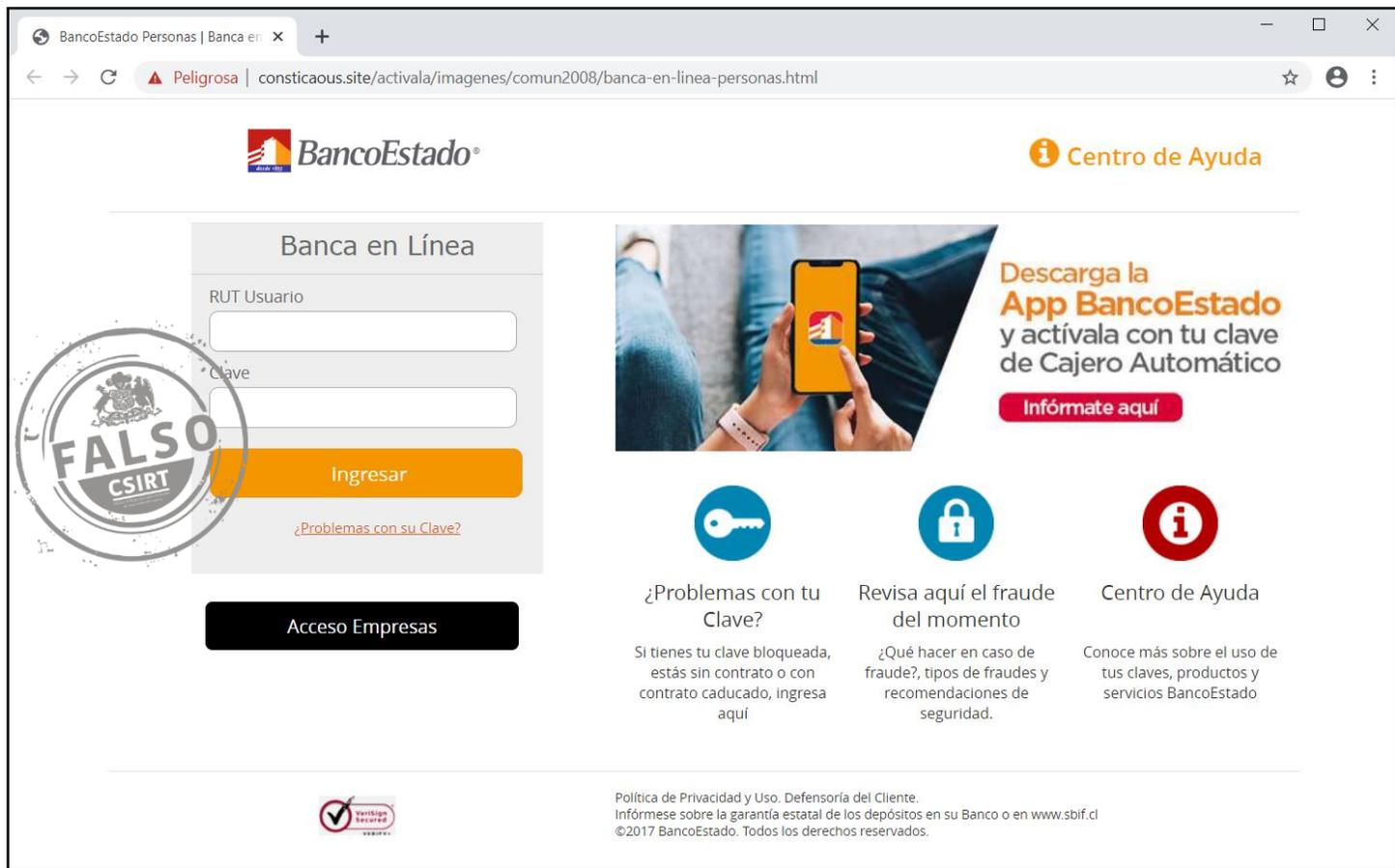
### Bono COVID-19 Chile de emergencia: ¿cómo obtener o actualizar el rut por internet **BancoEstado**?

Aplica terminos y condiciones [BancoEstado](#). Oferta valida desde 14 al 31 de Marzo ambas fechas inclusive, Sujeto a Evaluacion comercial.



Cronograma de pagos.

## Imagen del sitio



## 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.