

Alerta de seguridad informática	8FPH20-00242-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Junio de 2020
Última revisión	10 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 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 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 supuestamente proveniente del Banco Estado.

El atacante intenta persuadir a las personas para utilizar un enlace en el cuerpo del correo.

El mensaje del correo informa que se ha realizado una transferencia electrónica en la cuenta RUT de la persona con el abono de la pensión o beneficio IPS correspondiente al mes de mayo, así no tendrá que salir de casa.

La persona, al seleccionar el enlace para validar la transferencia, 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:

hxxp://bigforum[.]in/js/enviar.php?l=805038886

hxxps://bit[.]ly/3eMdIBf?l=www.bancoestado.cl

hxxps://petya.terytoriakrasy[.]com.ua/activacion/cuenta-zdgw/

### Urls sitio falso:

hxxps://www-bancoestado-cl.rocfmradio.fr/pagina/imagenes/comun2008/banca-en-linea-personas.html

### Smtip Host

[91.221.70.106]

### Sender

sn40@sites38.ru

### Asunto

Pensión del Mes de Junio.

## Imagen del mensaie



Estimado(a)

**BancoEstado**, le comunica a nuestros clientes afectados por la contingencia de los ultimos dias.

Le informamos que hoy,se ha realizado la Transferencia Electronica a su CuentaRut de la pension i beneficio IPS de mayo,para sus necesidades financieras.**Asi no tendras que salir de casa.**

Revisa tu Transferencia por este E-mail. [Aqui](#)

Si tienes consultas o deseas mas informacion,ingresa aqui:

[www.bancoestado.cl](http://www.bancoestado.cl)

[https://www.bancoestado.cl/Pension\\_Bono\\_IPS\\_Mayo](https://www.bancoestado.cl/Pension_Bono_IPS_Mayo)

Atentamente, BancoEstado.

Este es un correo electrónico generado automáticamente. Por favor no responder.



**Por tu seguridad, sigue estos consejos:**

- No compartas con terceros tus claves, tarjetas de coordenadas, códigos de verificación. BancoEstado nunca te pedirá información privada.
- Cuando gires en cajeros siempre revisa que no esté manipulado, que existan objetos extraños en el teclado, ranura o lector de tarjeta.
- Evita conectarte en redes libres o públicas para hacer transacciones bancarias o comprar por internet.

Conoce más recomendaciones de seguridad de BancoEstado en nuestro sitio [bancoestado.cl](http://bancoestado.cl)

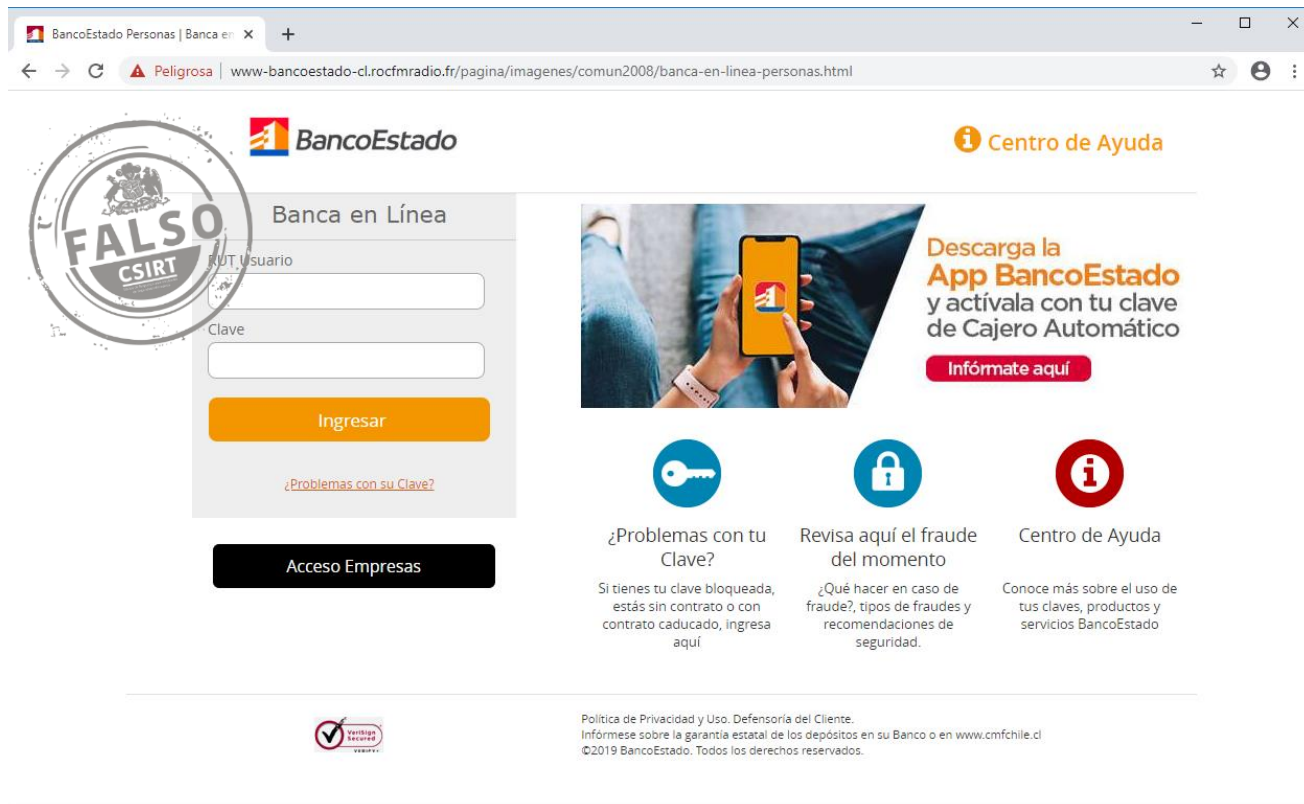
Síguenos en @bancoestado



De conformidad al artículo 28 B de la Ley 19.496 sobre Protección de los Derechos de los Consumidores, donde se regula el envío de correo masivos. Si usted no quiere recibir nuevos mensajes desde esta dirección, debe pinchar en el link al final de este correo para no recibir nuevos e-mail. Se deja constancia que los datos de contacto de este envío (direcciones, teléfonos, direcciones electrónicas, etc.) son reales y correctos y su e-mail ha sido extraído a través de medios mecánicos o tecnológicos desde nuestras propias bases de datos, sitios públicos de Internet e impresos de publicidad.

Si no deseas continuar recibiendo correos de BancoEstado, por favor haz click

## Imagen del sitio



BancoEstado Personas | Banca en línea

www-bancoestado-cl.rocmradio.fr/pagina/imagenes/comun2008/banca-en-linea-personas.html

**BancoEstado**

**Banca en Línea**

Usuario

Clave

**Ingresar**

[¿Problemas con su Clave?](#)

**Acceso Empresas**

**Centro de Ayuda**


**Descarga la App BancoEstado**  
y actívala con tu clave de Cajero Automático

**Infórmate aquí**

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

**Revisa aquí el fraude del momento**  
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.

**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.cmfchile.cl](http://www.cmfchile.cl)  
©2019 BancoEstado. Todos los derechos reservados.

## 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.