

| | |
|---------------------------------|-----------------------|
| Alerta de seguridad informática | 8FPH20-00318-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Octubre de 2020 |
| Última revisión | 19 de Octubre 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 atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica que por motivo de seguridad fue bloqueada su cuenta y que es necesario ingresar a su cuenta. Al seleccionar el enlace para ver más detalles es dirigido a un sitio falso, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirección:

[http://cetpline\[.\]com/Activacion/cuenta-dghq/](http://cetpline[.]com/Activacion/cuenta-dghq/)

Urls sitio falso:

[https://valpanet\[.\]com/pichanaki/pagina/imagenes/comun2008/banca-en-linea-personas.html](https://valpanet[.]com/pichanaki/pagina/imagenes/comun2008/banca-en-linea-personas.html)

Smtip Host

[45.7.230.89]

Sender:

apache@machine.net

Asunto

Fw: NOTIFICACION: CUENTA SUSPENDIDO

Otros antecedentes

URL Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

Certificado Digital

Fecha Valido : 23/07/2020
Fecha Término : 27/07/2021
Emitido : cPanel, Inc. Certification Authority

Datos Alojamiento

IP : 186.64.117.245
Número de sistema autónomo (AS) : 52368
Etiqueta del sistema autónomo : ZAM LTDA.
País : CL
Registrador : LACNIC

Datos del Dominio

Nombre de dominio : valpanet[.]com
Creado : 2014-07-12
Expira : 2021-07-12
Información del registrador : PDR Ltd. d/b/a PublicDomainRegistry.com
ID IANA : 303
Correo electrónico : No aplica
Servidores de nombres : ns1.sitiodns.net
ns2.sitiodns.net
ns3.sitiodns.net

Imagen del mensaje



Estimado(a) Cliente:



BancoEstado le informa que por motivos de seguridad bloqueamos su cuenta.

Es necesario que ingrese a nuestra web para poder verificar su información en nuestra base de datos o de lo contrario su servicio de banca por internet quedara bloqueada y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

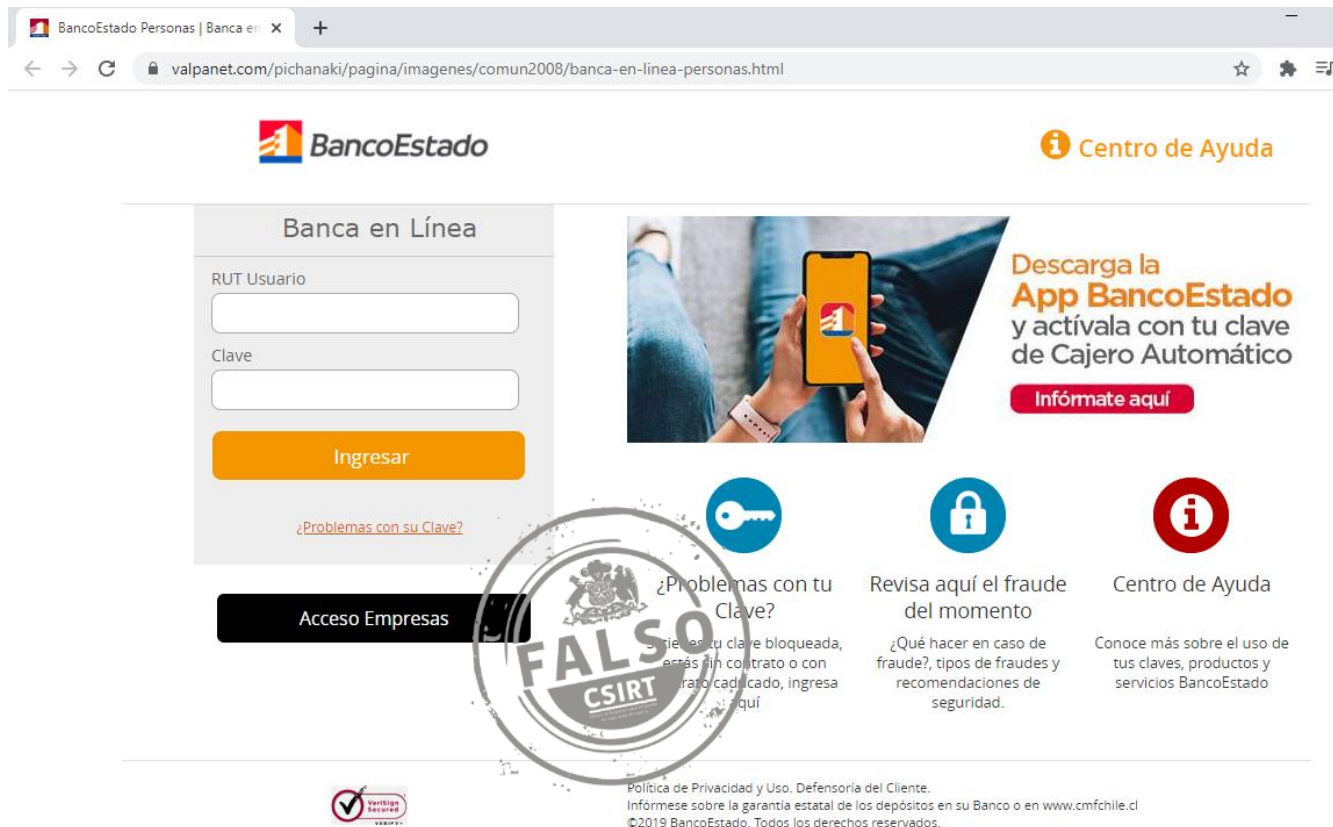
🏠 Ingresando a [Banco Estado - Activacion](#) Usted podra restablecer el acceso a sus cuentas

[\[\] \[Activar Cuenta\]](#)



© 2020 BancoEstado - todos los derechos reservados.
Informese sobre la garantía estatal de los depositos en su Banco o en www.sbif.cl

Imagen del sitio



The screenshot shows the login page for BancoEstado's online banking services. The browser address bar displays 'valpanet.com/pichanaki/pagina/imagenes/comun2008/banca-en-linea-personas.html'. The page features the BancoEstado logo, a 'Centro de Ayuda' link, and a login form with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for 'Problemas con su Clave?'. A large 'FALSO CSIRT' watermark is overlaid on the page. Below the login form, there are three service links: '¿Problemas con tu Clave?', 'Revisa aquí el fraude del momento', and 'Centro de Ayuda'. A footer section contains a 'Verifica Seguridad' logo, a privacy policy link, and copyright information for 2019 BancoEstado.

BancoEstado

Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

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

Infórmate aquí

¿Problemas con tu Clave?

Revisa aquí el fraude del momento

Centro de Ayuda

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