| | |
|---|---|
| **Alerta de seguridad informática** | 8FPH-00070-001 |
| **Clase de alerta** | Fraude |
| **Tipo de incidente** | Phishing |
| **Nivel de riesgo** | Alto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 02 de Noviembre de 2019 |
| **Última revisión** | 02 de Noviembre de 2019 |

**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), ha identificado una campaña de phishing a través de un correo electrónico cuyo mensaje intenta engañar a los usuarios del Banco Estado. El correo indica a la persona que lo recibe que, de acuerdo al Banco, la cuenta arroja un error, lo que el sistema entiende como “cuenta suspendida”. La razón sería un supuesto proceso de validación de identidad pendiente por parte del usuario, acción que los estafadores facilitan de realizar a través de un enlace en el correo. Cuando la víctima ingresa al vínculo, se expone al robo de sus credenciales desde un sitio semejando al del Banco.

**Observación**

Solicitamos tener en consideración las señales de compromiso en su conjunto

**Indicadores de compromisos**

**Url's:**

http[:]//greatfootball[.]club/readme/Simuladores/
http[:]//scratchpad.co[.]in/readme/imagenes/comun2008/banca-en-linea-personas[.]html

**Smtp Host**

Practika[.]net [45[.]236[.]129[.]230]
hwsrv-624221[.]hostwindsdns[.]com [192[.]119[.]119[.]64]

**Sender**

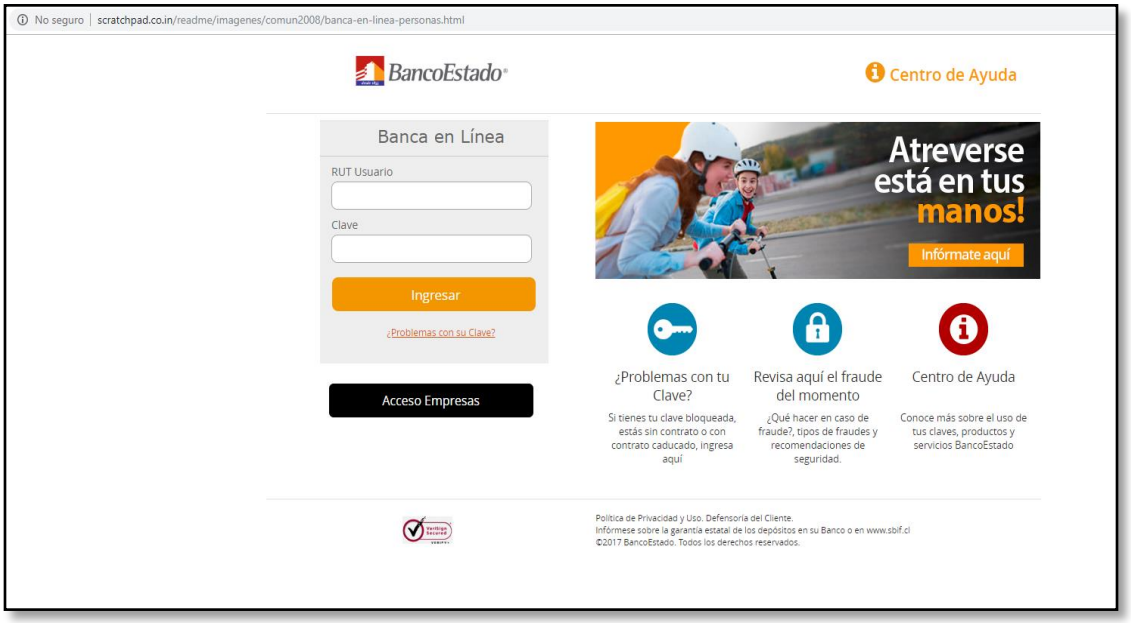
apache@practika[.]net
apache@hwsrv-624221[.]hostwindsdns[.]com

**Subject:**

✓ Fw: Notificacion- Cuenta Bloqueada

**Imagen Phishing Correo**

**Imagen Sitio Web**




**Recomendaciones**

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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 que sean los oficiales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.02 19:10:37 -03'00'