

| | |
|---------------------------------|---------------------|
| Alerta de seguridad cibernética | 8FPH20-00160-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de Abril de 2020 |
| Última revisión | 07 de Abril 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 SMiShing a través de un mensaje de texto que intenta engañar a los usuarios del Banco ITAU.

El atacante envía un mensaje señalando a quien lo recibe, que su cuenta bancaria de se encuentra desvinculada en el sistema. Para solucionar el inconveniente, se deben actualizar los datos en un enlace adjunto. De seleccionar el enlace, la víctima es dirigida a un sitio semejante al del Banco. De esta forma el atacante captura las credenciales de la persona.

CSIRT agradece la colaboración de Nicolle Bravo, (@NicolleABG) quien informó de este SMiShing a través de nuestro twitter. Y recordamos a todos quienes siguen nuestros informes que para reportar un incidente, lo pueden hacer en el formulario de nuestro sitio web www.csirt.gob.cl o al teléfono +(562) 2486 3850, las 24 horas del día.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls sitio falso:

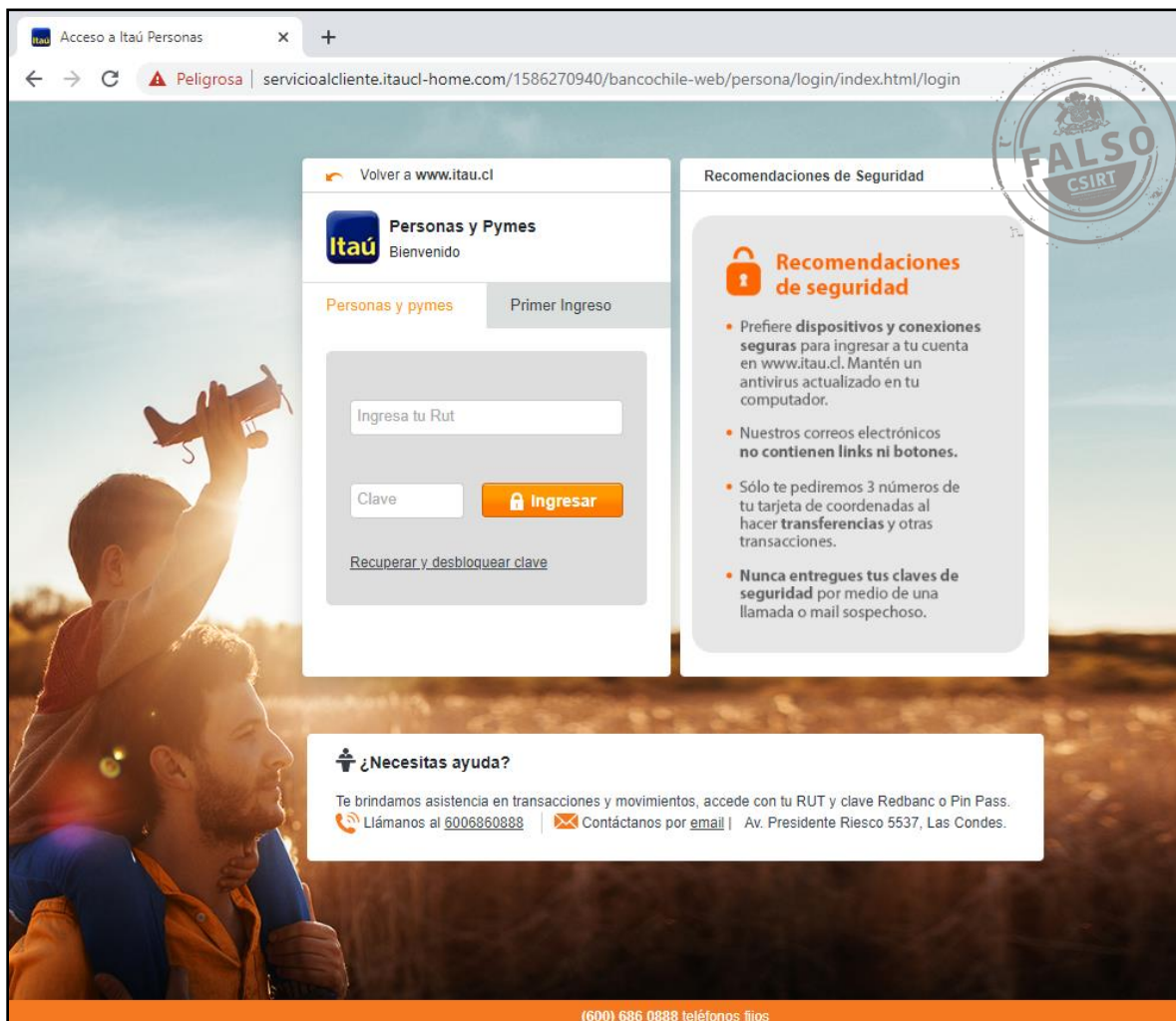
<https://servicioalcliente.itauc-home.com/1586270940/bancochile-web/persona/login/index.html/login>

IMAGEN DEL MENSAJE

Banco Itau - Su cuenta se encuentra desvinculada en nuestro sistema, para solucionar inconvenientes y bloqueos, actualice sus datos aquí: <https://tr.im/itau>



IMAGEN DEL SITIO



Acceso a Itau Personas

Peligrosa | servicioalcliente.itauc.cl-home.com/1586270940/bancochile-web/persona/login/index.html/login

Volver a www.itauc.cl

Personas y Pymes
Bienvenido

Personas y pymes Primer Ingreso

Ingresa tu Rut

Clave

[Recuperar y desbloquear clave](#)



Recomendaciones de Seguridad

Recomendaciones de seguridad

- Prefiere **dispositivos y conexiones seguras** para ingresar a tu cuenta en www.itauc.cl. Mantén un antivirus actualizado en tu computador.
- Nuestros correos electrónicos **no contienen links ni botones**.
- Sólo te pediremos 3 números de tu tarjeta de coordenadas al hacer **transferencias** y otras transacciones.
- **Nunca entregues tus claves de seguridad** por medio de una llamada o mail sospechoso.

¿Necesitas ayuda?

Te brindamos asistencia en transacciones y movimientos, accede con tu RUT y clave Redbanc o Pin Pass.

 Llámarnos al [6006860888](tel:6006860888) |  Contáctanos por [email](mailto:) | Av. Presidente Riesco 5537, Las Condes.

(600) 686 0888 teléfonos fijos

FALSO
CSIRT

RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
 - Desconfiar de los enlaces y archivos en los mensajes o correo.
 - Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
 - Prestar atención en los detalles de los mensajes o redes sociales
 - Mantener sus dispositivos actualizados
 - Mantener las aplicaciones actualizadas
 - Desconfiar de promociones que no se encuentren en los canales oficiales
- Siempre visitar los canales de comunicaciones oficiales