

Alerta de seguridad informática	8FPH21-00427-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de agosto de 2021
Última revisión	17 de agosto de 2021

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 afectada 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 de Gobierno) advierte sobre una campaña de phishing que está siendo difundida a través de un correo electrónico que se hace pasar como proveniente del Banco Itaú.

El atacante busca persuadir a las personas de utilizar un enlace contenido en el cuerpo del correo. Para lograr eso, el mensaje del email informa falsamente que la cuenta del cliente requiere una actualización. Si hacen clic en el enlace, las personas son dirigidas a un sitio falso, donde se exponen al robo de datos confidenciales.

Observación

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

Indicadores de compromiso

URL sitio falso:

[https://app.itau-cl.com/choose\[.\]php](https://app.itau-cl.com/choose[.]php)

URL redirección

<https://www.atrilcom.com/wp-admin/js/>

Asunto:

Nueva notificación de envío de DHL 3856210210

Seguimiento de su envío: 6540674221

Shipment Notification 📧 75952666522

Correo electrónico

[www-data@city.hokota.ed\[.\]jp](mailto:www-data@city.hokota.ed[.]jp)

[kourify@host.yourownnameserver\[.\]com](mailto:kourify@host.yourownnameserver[.]com)

[listsurge@server.layerstech\[.\]com](mailto:listsurge@server.layerstech[.]com)

SMTP Host

[222.230.107.59]

[95.216.76.116]

[199.201.88.128]

Otros antecedentes

Certificado Digital

Fecha Valido : 05-07-2021
Fecha Término : 04-10-2021
Emitido : cPanel, Inc. Certification Authority

Datos Alojamiento

IP : [50.31.134.90]
Número de sistema autónomo (AS) : 23352
Etiqueta del sistema autónomo : Servercentral
País : US
Registrador : ARIN

Datos del Dominio

Nombre de dominio : itau-cl[.]com
Creado : 15-08-2021
Expira : 15-08-2022
Información del registrador : PDR Ltd. d/b/a PublicDomainRegistry.com
ID IANA : 303
Correo electrónico : abuse-contact@publicdomainregistry.com
Servidores de nombres : kinghostbr.earth.orderbox-dns.com
kinghostbr.mars.orderbox-dns.com
kinghostbr.mercury.orderbox-dns.com
kinghostbr.venus.orderbox-dns.com

Imagen del mensaje



Aviso mediante notificación. **Itau - Sistema de seguridad integrado.**

Notificación de Itau - Sistema Integrado.



Estimado cliente Letitia Alejandra, llegamos a través de esta notificación vía correo electrónico para notificarle sobre las condiciones de su cuenta en nuestra institución.

Su cuenta está fuera del período permitido de actualización de registro. Por estos motivos, es necesario actualizar sus datos personales utilizados en su cuenta.

Este proceso es necesario para mantener sus datos actualizados y siempre seguros. Realice el proceso requerido haciendo clic en el botón de abajo. El proceso se realiza de forma totalmente online, sin necesidad de acudir personalmente a una de nuestras instituciones, respetando así los protocolos de seguridad y distancia.

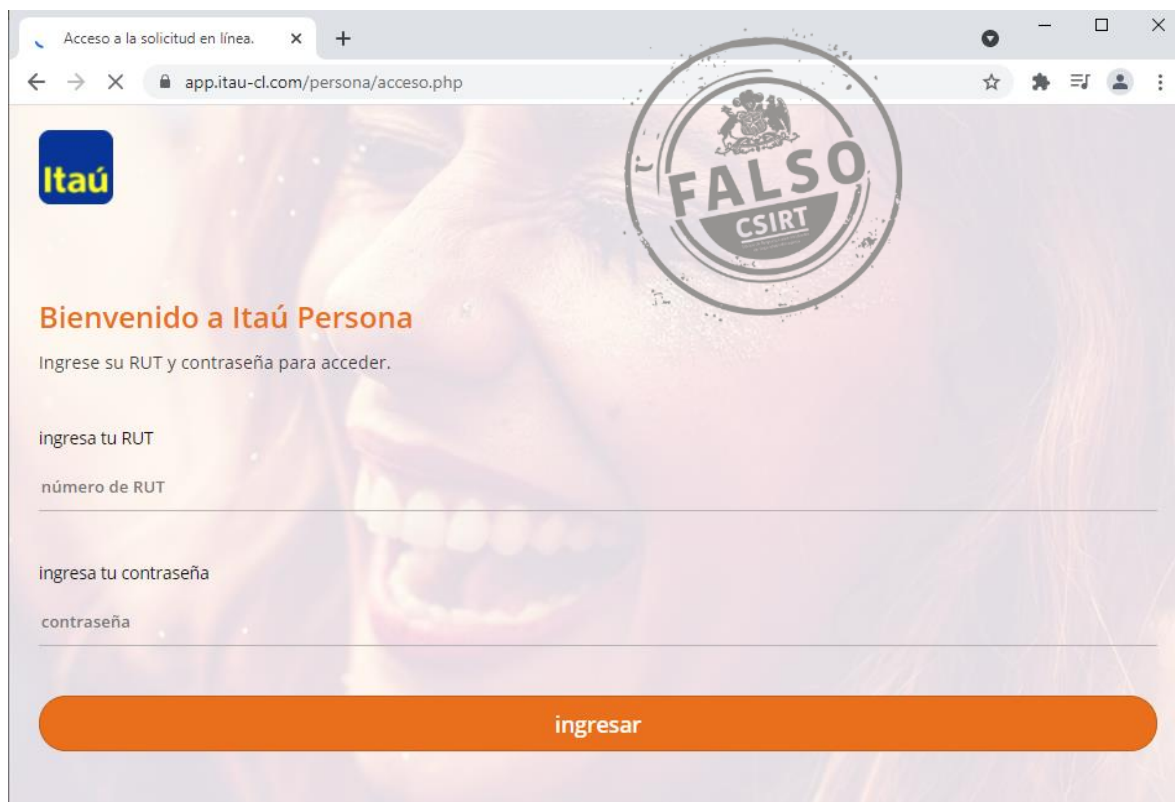
Regularizar datos

Este proceso es importante para el buen funcionamiento de su cuenta y la seguridad de sus datos de registro. Si el proceso no se lleva a cabo, nuestro sistema de seguridad automatizado puede suspender temporalmente su cuenta.

© 2021 - Itau - Chile.
Todos los derechos reservados. Sistema de notificación en IñfÁnea.

17/08/2021 02:21:01

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.