CAS-CHILE®
LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

¿Cómo protegerse de los ataques de Phishing?

SGSI
CAS-CHILE

¿Qué es el PHISHING?

Es una **técnica de ciberdelincuencia** y una **forma de engaño más común** que emplea la suplantación de identidad, el engaño y el fraude para manipular a las víctimas y obtener información personal confidencial.

Los autores del phishing no tratan de explotar una vulnerabilidad técnica en el sistema operativo de su dispositivo, sino que utilizan "ingeniería social".

La Ingeniería social es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño

"El phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva".

¿Cómo funciona el phishing?

El ataque se realiza mediante comunicaciones electrónicas.

El atacante se hace pasar por un tercero

Sea persona u Organización de Confianza

El objetivo del phishing es obtener información personal confidencial.

Datos personales

- Número de documento de identidad
- Direcciones de correo electrónico
- Datos de localización y contacto

Información financiera

- Número de cuentas o tarjetas bancarias

Credenciales de acceso

- Cuentas de correo
- Redes sociales

Medios que utiliza el Phishing

Como ya hemos visto, los ataques de phishing pueden realizarse a través de diferentes vías:

Phishing por correo electrónico

Es el método más habitual. Estos mensajes suelen incluir un enlace hasta un sitio web malicioso o archivos adjuntos infectados con malware.

Phishing por sitio web

Son copias falsas y muy similares de sitios web que el usuario conoce y en los que confía. El objetivo es que el usuario introduzca sus datos de inicio de sesión.

Phishing por teléfono

También llamado 'vishing', en esta modalidad de phishing el atacante intenta engañar a la víctima por teléfono.

Phishing por SMS

El 'smishing' se realiza a través de mensajes de texto en donde se incluyen enlaces que descargan en el teléfono un malware para robar la información personal.

Phishing por redes sociales

Es el método más novedoso y consiste en enviar mensajes directos a través de redes sociales con enlaces poco fiables.

Ciberataques:

¿Cuáles son las repercusiones que podemos tener?

En función del tipo de ciberataque y de la víctima, te mencionamos las repercusiones más habituales

CAS-CHILE®

¿Conoces todo lo que puede hacer el ciberdelincuente con tu correo electrónico?

- El correo electrónico es el centro de tu existencia digital, por lo que está vinculado con tu banco, redes sociales y muchos más

Acceder información importante

- Si saben que plataforma usas podrían incluirte en listas de Spam personalizadas o incluso ataques phishing

Conocer las plataformas y servicios que utilizas

- Puedan que sea contactos de tu directorio o cualquier otra persona

Atacar a otros

- Pueden fácilmente contactar a otros en tu nombre si ingresan con tu correo electrónico

Suplantar tu identidad

- El correo electrónico funciona prácticamente como un gestor de claves

Usar contraseñas de otros servicios

¿Cómo reconocer un ataque de phishing?

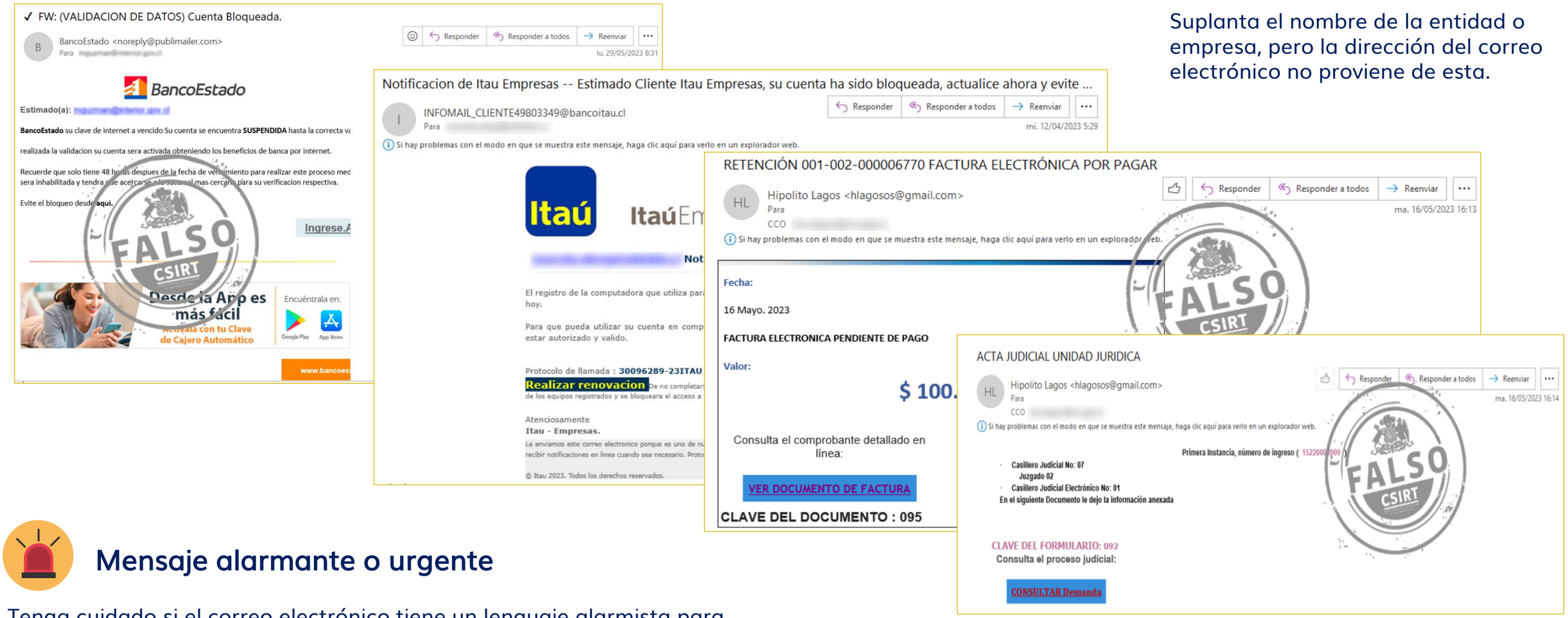
- **INCLUYE contenido alarmante o urgente**, ya sea en asunto o contenido del mensaje.
- **SOLICITA información confidencial**: Confirmación de cuenta, contraseñas, información personal o realizar un pago.
- **ADJUNTA documentos** o información no solicitada: como facturas o cotizaciones
- **TIENE faltas de ortografía** o imágenes de mala calidad.
- **TIENE un remitente desconocido** y que no proviene de la empresa aludida
- **CONTIENE enlaces extraños** adjuntos.

CAS-CHILE®
LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

SGSI
CAS-CHILE

Casos reales de Phishing

➢ Ejemplo de Phishing por correo electrónico:



Remitente desconocido

Suplanta el nombre de la entidad o empresa, pero la dirección del correo electrónico no proviene de esta.

Mensaje alarmante o urgente

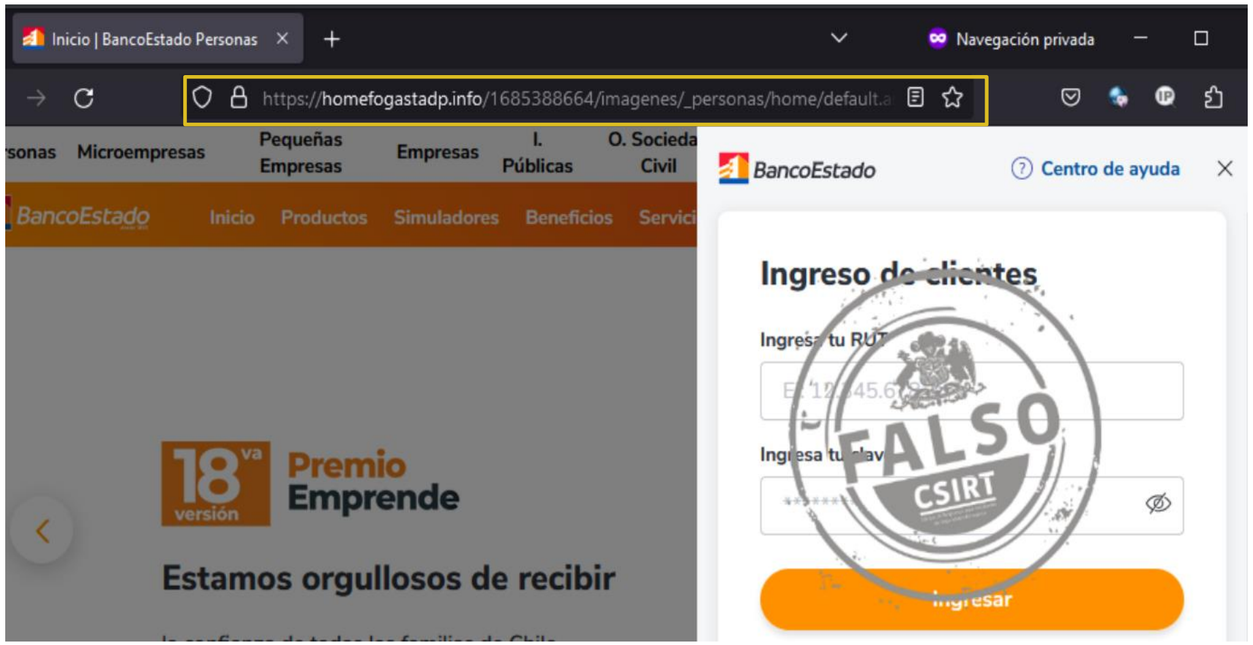
Tenga cuidado si el correo electrónico tiene un lenguaje alarmista para crear un sentido de urgencia, instándole a que haga clic y “actúe ahora”

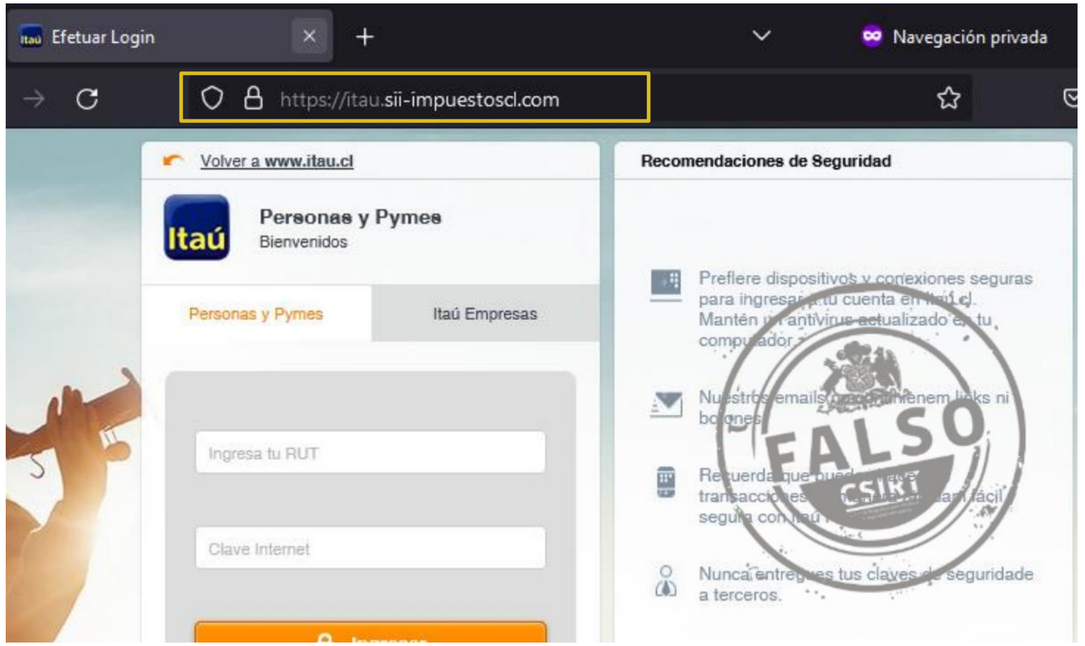
➢ Sitios Web falsos:

Si de todos modos ingresas al link adjunto al correo, probablemente llegarás a algo que, a simple vista, parece ser la página de la institución aludida.

Pero cuidado, antes de ingresar tus datos personales (como usuario, claves y números de tarjeta), revisa la dirección del sitio web para saber si estás realmente en el sitio de tu institución.

Es recomendable nunca hacer clic en enlaces que dicen ser de tu banco o cualquier empresa que te ofrece servicios, sino ingresar directamente el nombre de su web oficial en la barra de direcciones de tu navegador web.





Las imágenes muestran sitios web falsos, pero gráficamente no parecen sospechosos a simple vista.

¿En qué fijarse? Siempre, revisa la dirección web.

Phishing con malware (programa o código malicioso)

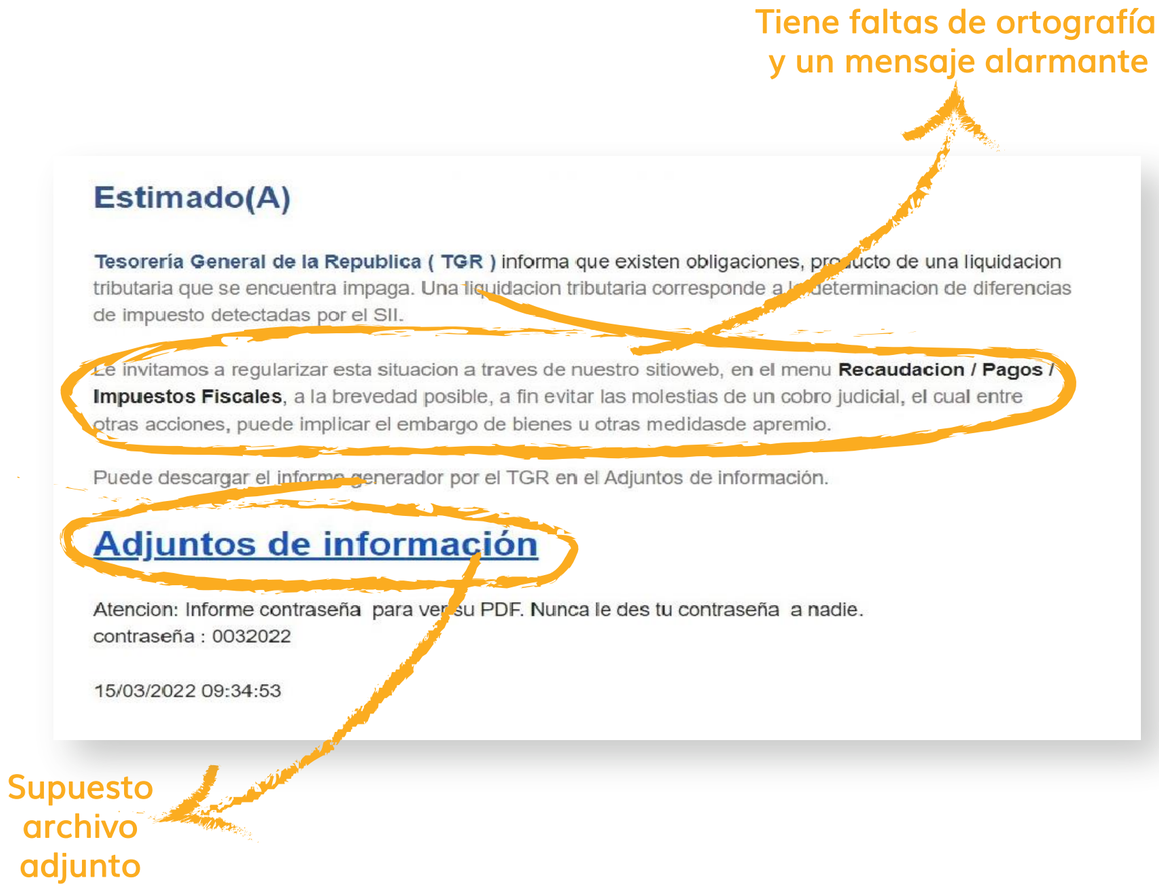
Los phishing con malware buscan causar daño a cualquier clase de dispositivo, como computadoras, celulares, toda la infraestructura de red, etc.

Existen distintos tipos de malware y cada uno tiene características y formas de propagarse diferentes. Así como sus consecuencias son variadas dependiendo el tipo de infección, por ejemplo:

- Anuncios molestos
- Robo de datos personales o sensibles
- Envío de correos sin consentimiento
- Pérdida del control del equipo.
- Cifrado de archivos (para pedir recompensa, ataque conocido como ransomware)

Para lograr que sus víctimas descarguen estos archivos maliciosos, los delincuentes adjuntan supuestos documentos importantes para el receptor del mensaje.

Así por ejemplo, ocurre en el caso de los correos que suplantan la identidad de la Tesorería General de la República, en los que señalan falsamente que existirían obligaciones impagas, como muestra la imagen:



CAS-CHILE®
LÍDER EN SOFTWARE DE GESTIÓN PÚBLICA

SGSI
CAS-CHILE

Recomendaciones para prevenir un ataque de Phishing

Buenas prácticas de seguridad

Desconfía de los correos y SMS que provienen de fuentes desconocidas

Confirma antes de actuar. Las empresas auténticas nunca contactarán por correo electrónico o teléfono para solicitar datos personales

No abrir archivos ni utilizar enlaces contenidos en un correo enviado por un remitente desconocido o que no estabas esperando, sospecha.

- Antes de hacer clic en el enlace coloca el cursor del mouse sobre el hipertexto para ver la URL a la que nos redirige
- Bajo ningún contexto descargues archivos adjuntos si no puedes confirmar que se trata de un mensaje legítimo.

Verifica el certificado digital del sitio web y comprueba que la URL sea de los sitios oficiales.

- Por ello escribe la dirección web del sitio directamente en el navegador ante sospechas u no ingreses desde el link adjunto al correo.
- Nunca ingresar contraseñas si no confías en un sitio web.

Buenas prácticas de seguridad

Revisa el contenido, y trata de entender el propósito real del correo o mensaje y que acciones te piden.

Prestar atención en los detalles :

- ¿Insisten en hacer **clic en un link o adjunto**?
- ¿Están pidiendo algo fuera de lo normal? ¿Es un **procedimiento habitual**?
- ¿Hay alguna **referencia personal** hacia ti (nombre, número de teléfono, etc.) o es un correo o mensaje genérico?
- ¿Utilizan un **tono alarmante, amenazante** o esta ofreciendo algo?
- ¿El mensaje escribe con **faltas de ortografía, errores gramáticas**, palabras no muy comunes o traducciones mal hechas?

Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por Internet.

- Si son muy buenas, duda e ingresa desde los sitios web directo y no desde un link adjunto.
- Cuidado con los sitios web, siempre revisa las URL

Mantener actualizadas sus plataformas

Mantener el software actualizado es de fundamental importancia ya que es el único modo de evitar problemas de vulnerabilidades y de mejorar las funciones de las aplicaciones de nuestros dispositivos.

El phishing se crea, pero no se destruye, solo se transforma

Existen infinitas posibilidades para que los ciberdelincuentes lleven a cabo sus campañas de ciberataques y con el paso del tiempo estas se vuelven más sofisticadas y aumentan las posibilidades de caer en ellas.

Las técnicas utilizadas por los criminales se adaptan a las necesidades de los usuarios, es decir, dependiendo de la época del año, abundan unas modalidades de phishing u otras.

Por tanto, se puede decir que los ciberdelincuentes se mimetizan con los acontecimientos temporales y sociales.

Todos jugamos un papel fundamental en la protección y seguridad de nuestra información para protegernos de ciberataques.

Proteger la información que maneja de empresa no solo depende del Área de Infraestructura TI, tus acciones pueden proteger o perjudicar las operaciones de la empresa.

CAS-CHILE® conecta a las
Municipalidades del País.