ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

Cómo identificar phishing, malware y sitios falsos

Ramón Rivera Notario
Agencia Nacional de Ciberseguridad (ANCI)

El phishing

El phishing

Este es un tipo de ataque informático que engaña a su víctima para convencerla, sin que esta se de cuenta, de que descargue un programa malicioso, envíe dinero o entregue datos personales.

El phishing

Los delincuentes mandan un email, SMS o WhatsApp a la víctima haciéndolo pasar por una comunicación legítima, suplantando a personas o instituciones confiables.

Si la víctima confía, puede descargar malware, acceder a una página maliciosa, entregar sus datos bancarios o información confidencial, entre otros.

Peligros del phishing: malware

Malware o código malicioso: Son programas que tienen como objetivo realizar algún efecto dañino en un sistema. Es lo que antes se llamaba simplemente un virus.

Formas de infección:

- Enlaces y URL maliciosos.
- Pendrives infectados.
- Troyanos.
- Movimiento lateral: Delincuentes ganan acceso a un equipo en la organización, y desde ahí van ganando privilegios a otras partes de esta.

Peligros del phishing: revelación de información

Otro uso malicioso del phishing es conseguir datos confidenciales de la víctima o la organización en la que trabaja.

Ejemplos:

- **Robo de cuentas en apps**: Delincuentes contactan a una persona por WhatsApp, Instagram, Facebook u otras aplicaciones y les piden, con engaños, su código de recuperación de la cuenta.

- **Fraude en empresas:** Malhechores contactan a un empleado haciéndose pasar por una de sus jefaturas, o por una organización diferente que trabaja con su empleador. Con engaños piden datos, generalmente de forma urgente, para que no consulten con otros empleados. Incluso pueden conseguir que la víctima autorice pagos o entregue datos confidenciales.

El phishing y la psicología humana

Estos ataques se aprovechan de nuestra naturaleza, con técnicas para que no pensemos antes de responder o hacer clic.

- Exige una respuesta urgente.
- Dice provenir de una jefatura o autoridad.
- Llaman a la solidaridad, a la curiosidad o a la codicia del destinatario.

Un ejemplo común es la “estafa del príncipe nigeriano”, en la que el delincuente dice ser millonario y necesitar sacar dinero de su país.

- Cuando se hace por SMS, se conoce como “smishing”

- Si es llamada, es un “vishing” (la v viene de “voz”).

- Y cuando es a través de un código QR, les llaman quishing.

El phishing

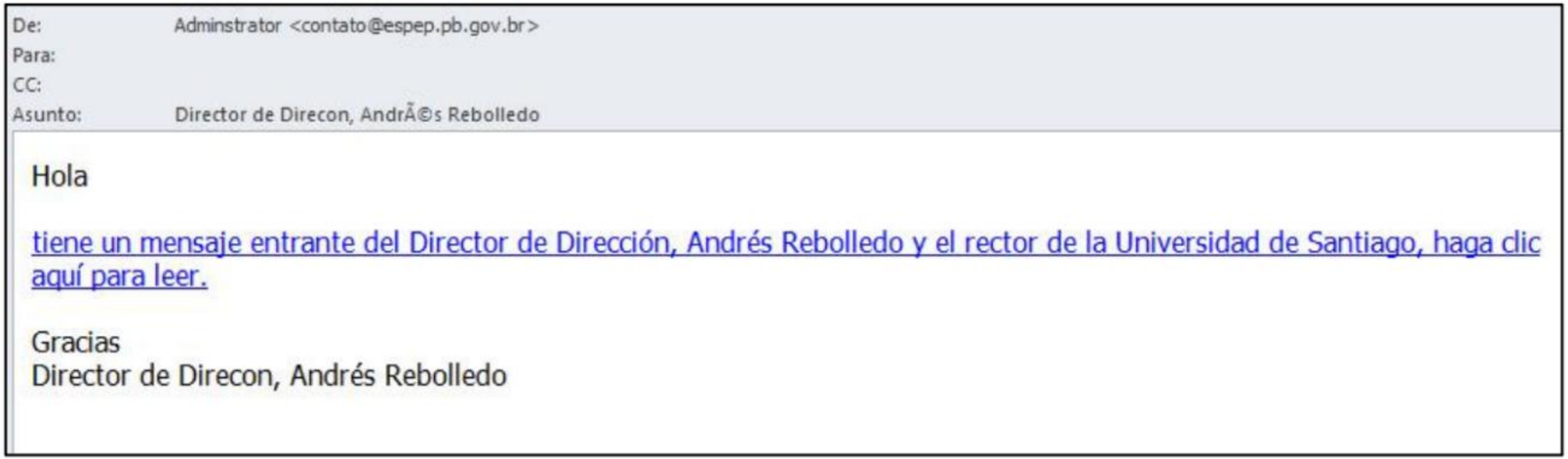

ROYAL BANK
of
NIGERIA
He escrito a todos quienes pude encontrar, mi Príncipe, pero nadie quiere ayudarlo a mover su dinero
AGENT-X COMICS
WWW.AGENT-X.COM.AU

Características de un phishing

Se suelen dar una o varias de estas características:

1. Pide que se descargue o abra un archivo adjunto, muchas veces señalando que es una factura o una citación judicial.

2. Dice provenir de una persona o institución de confianza o importancia.


De: Adminstrator <contato@espep.pb.gov.br>
Para:
CC:
Asunto: Director de Direcon, AndrÃ©s Rebolledo

Hola

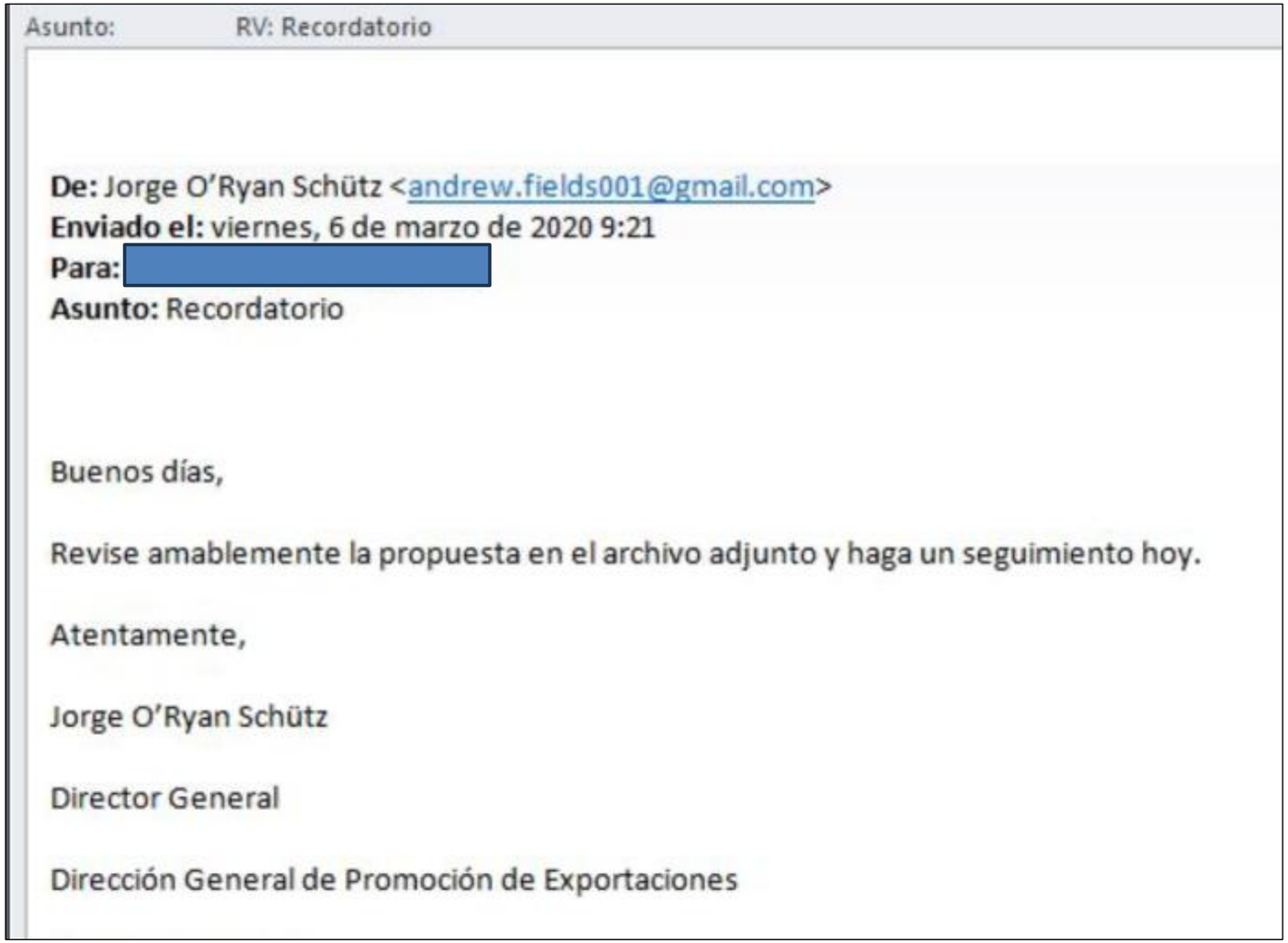
tiene un mensaje entrante del Director de Dirección, Andrés Rebolledo y el rector de la Universidad de Santiago, haga clic aquí para leer.

Gracias
Director de Direcon, Andrés Rebolledo

Características de un phishing

Se suelen dar una o varias de estas características:

3. Se insta al receptor a actuar ya.



Asunto: RV: Recordatorio

De: Jorge O'Ryan Schütz <andrew.fields001@gmail.com>
Enviado el: viernes, 6 de marzo de 2020 9:21
Para: [redacted]
Asunto: Recordatorio

Buenos días,

Revise amablemente la propuesta en el archivo adjunto y haga un seguimiento hoy.

Atentamente,

Jorge O'Ryan Schütz

Director General

Dirección General de Promoción de Exportaciones

Características de un phishing

Se suelen dar una o varias de estas características:

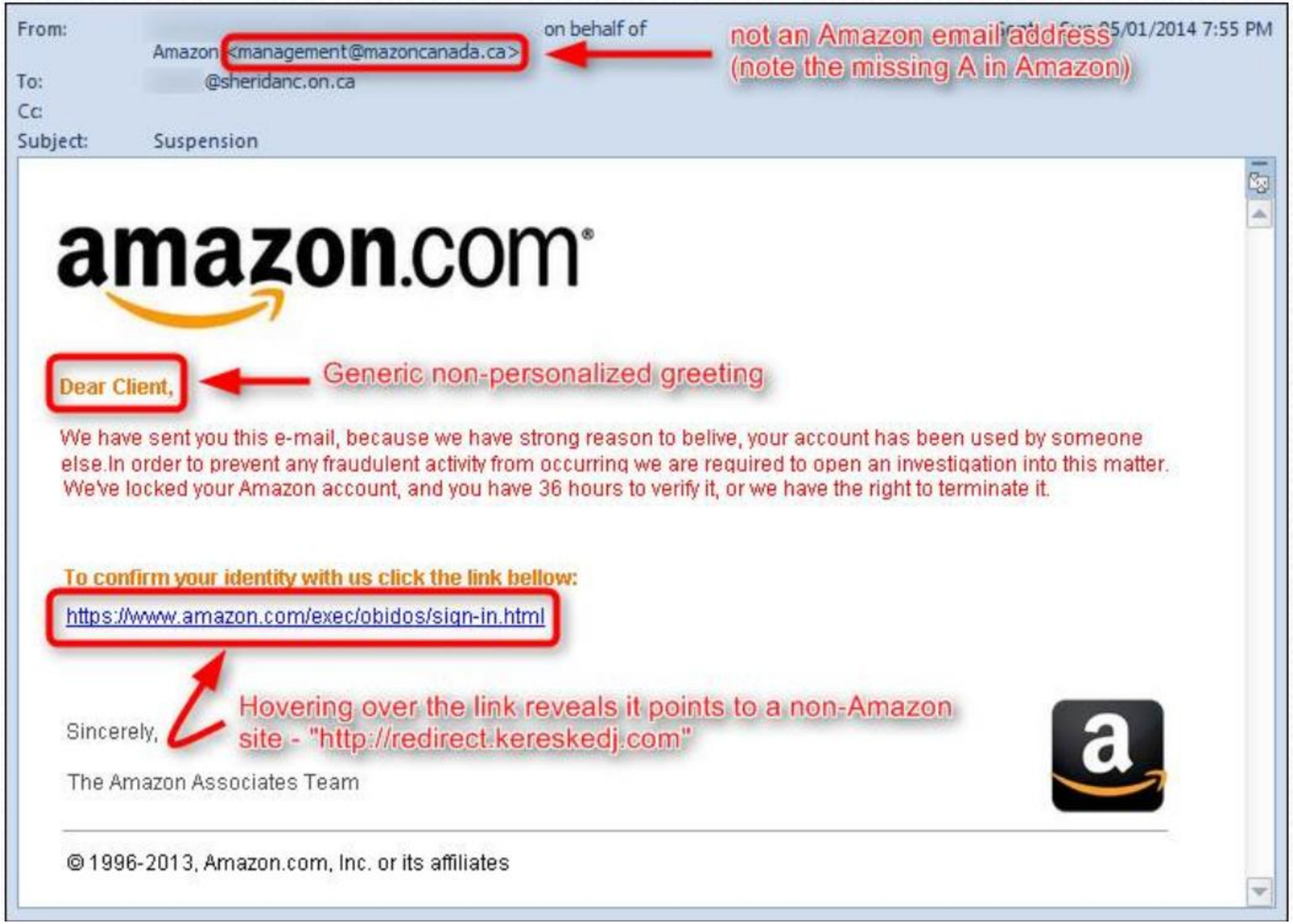
4. La dirección del remitente no coincide con quien dice ser, o la institución a la que dice pertenecer.

5. Se dirigen al destinatario de forma impersonal (“cliente”).

6. Los enlaces tienen un texto falso o la URL ofuscada.

7. Faltas de ortografía.

Características de un phishing



Ejemplos

Ha recebido un nuevo documento eletrónico. Fecha Documento: 30-01-2025

"Construccion Y Reparciones - Equipo de finanzas" <support@fsv-volleyball.de>
Para [redacted]

Responder | Responder a todos | Reenviar | ...

lun 20-01-2025 6:16

Construccion Y Reparciones Varias

Estimado/a [redacted]

Ha recebido un nuevo documento eletrónico.

- Tipo: Factura Eletronica
- Folio Nro: 5495856734543007
- Fecha Documento: 30-01-2025
- Monto Total: $ 438.000

En el siguiente botón podrá ver y descargar su visor documento electónico.

Ver Documento

(.msi) (Para ver su factura, deberá instalar el visor de facturas Windows, no disponible para dispositivos móviles.)

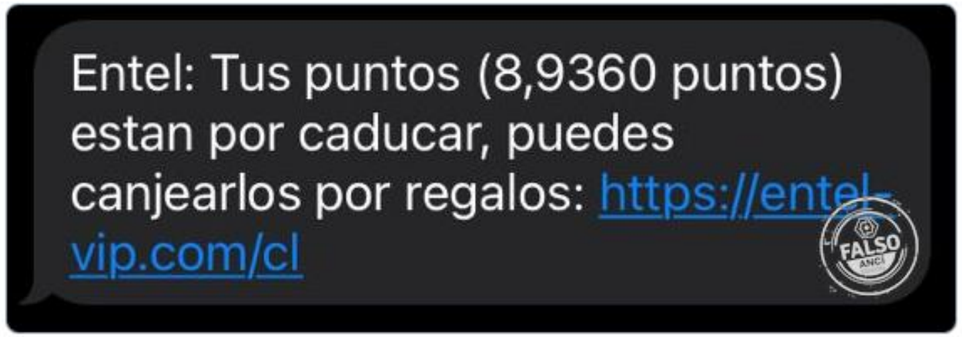
Gracias
Equipo de finanzas

Esta notificación ha sido generada automáticamente cumpliendo los más altos estándares de seguridad con certificaciones AWS y certificación ISO 27001

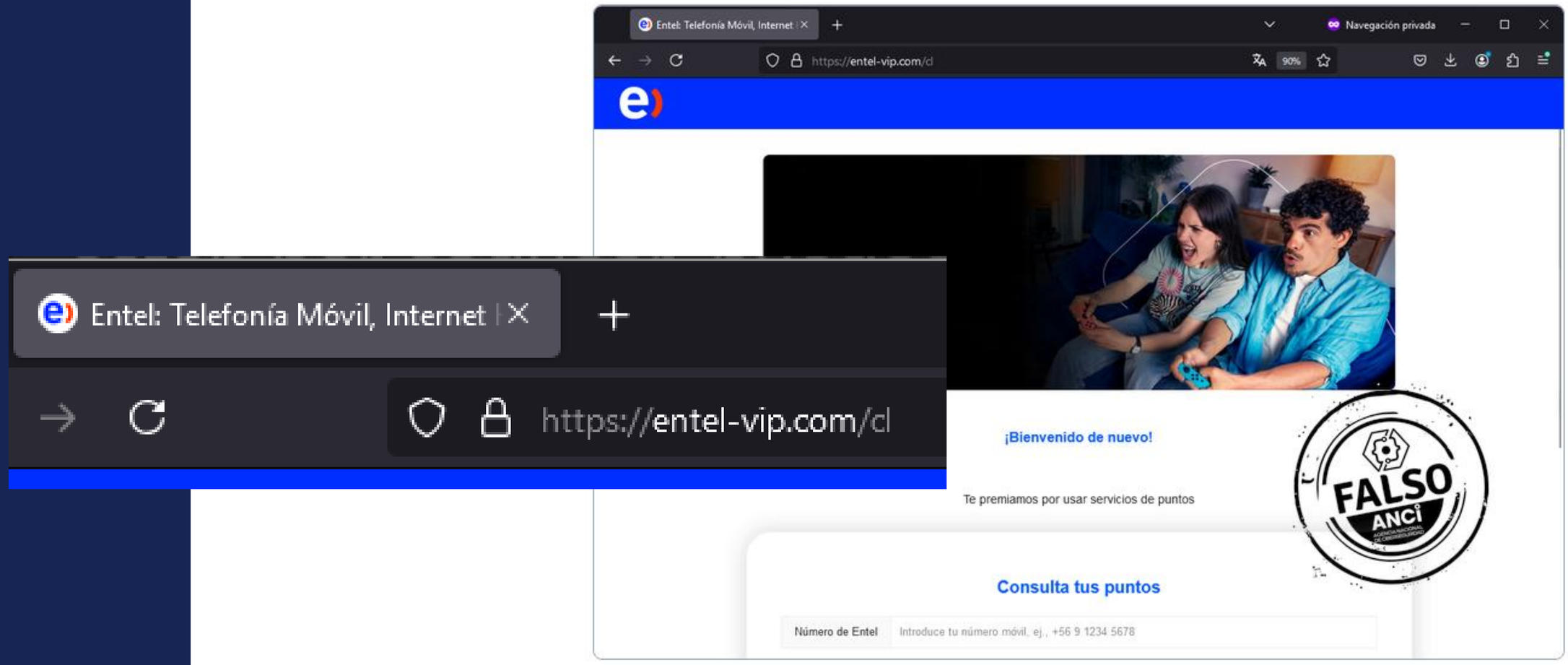
Sus mensajes personales están protegidos con la criptografía de punta a punta.

Este ejemplo de phishing descarga un malware que roba datos, llamado Mekotio.

Ejemplos

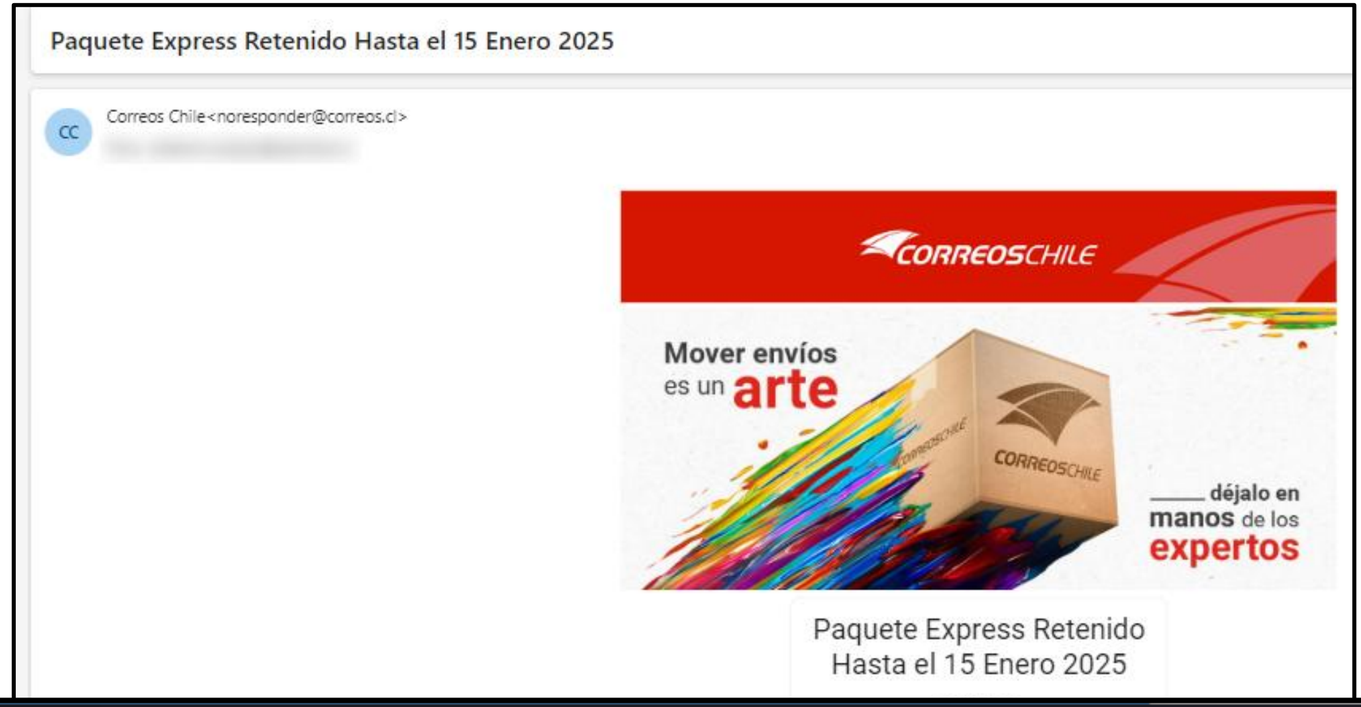


Evidencia 1:



Evidencia 2:

Ejemplos


Paquete Express Retenido Hasta el 15 Enero 2025
CC
Correos Chile<noresponder@correos.cl>
CORREOSCHILE
Mover envíos
es un arte
déjalo en
manos de los
expertos
Paquete Express Retenido
Hasta el 15 Enero 2025

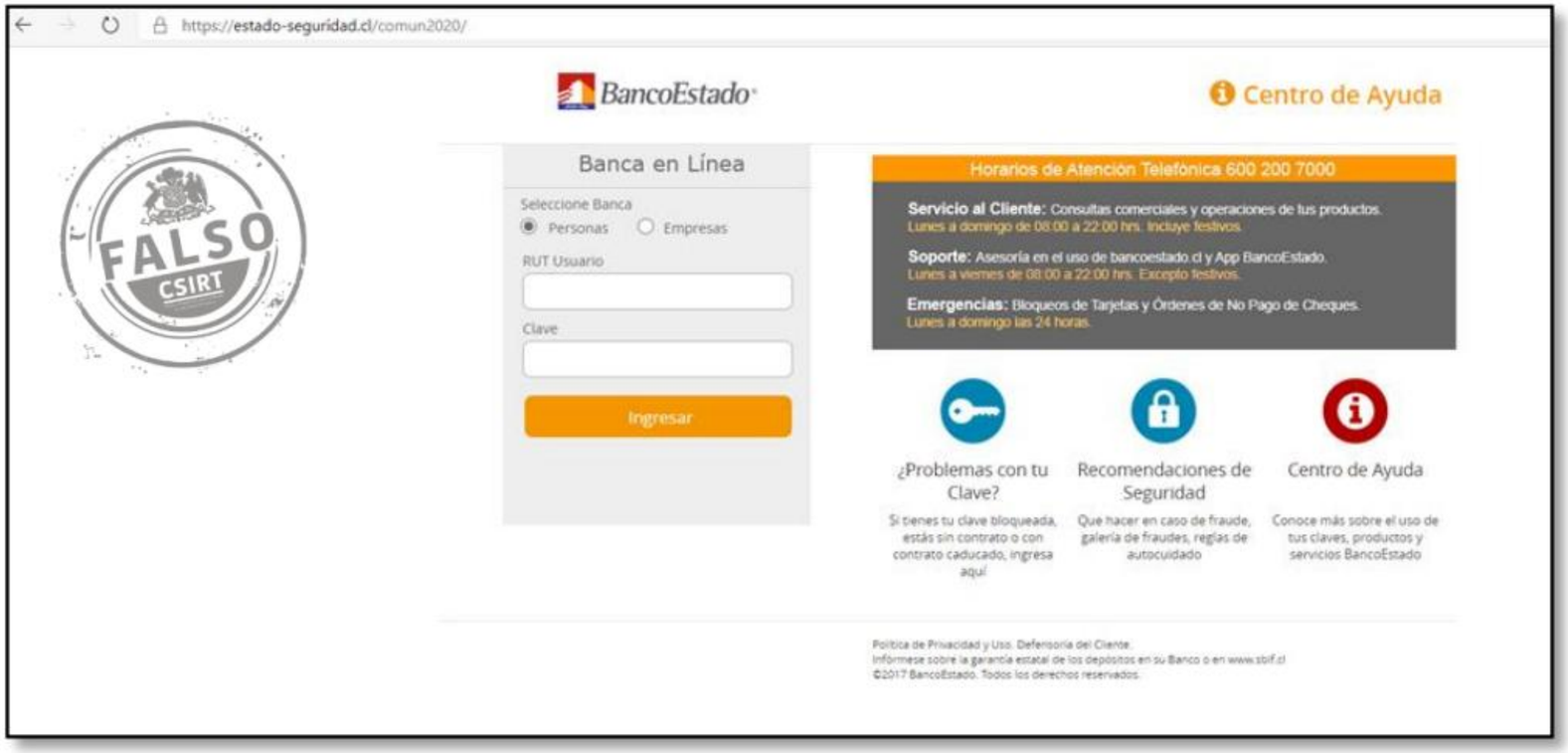

Seguimiento en Línea - Correos
Navegación privada
correoschile.chile-cl.site/seguimiento/seguimiento/datos.html
90%
Persona
Empresas
CORREOSCHILE
Herramientas
Servicios
Internacional
Emprendedores
Ayuda
Ingresar
Envíos en curso 1
Entregado 0
No Entregado 1
Dirección de envío
Estimados clientes, nos tomamos muy en serio la prevención del fraude. Para garantizar que se verifique su identidad, le pedimos que vuelva a ingresar su dirección de envío. para completar su entrega
Estado
Envío sin confirmar
Seguimiento N°
SM00C45E709
Guardar

Ejemplos

BANCO ESTADO informa que hemos detectado un dispositivo no frecuente evite que tu cuenta no sea SUSPENDIDA verifica aqui:https://estado-seguridad.cl/comun2020/ 0:36

FALSO CSIRT

IMAGEN DEL SITIO



De: zimbra <zimbra@sssdefensa.cl>
Fecha: 3 de julio de 2017, 04:54:22 CLT
Para: [redacted]
Asunto: Actualizacion de politicas de seguridad

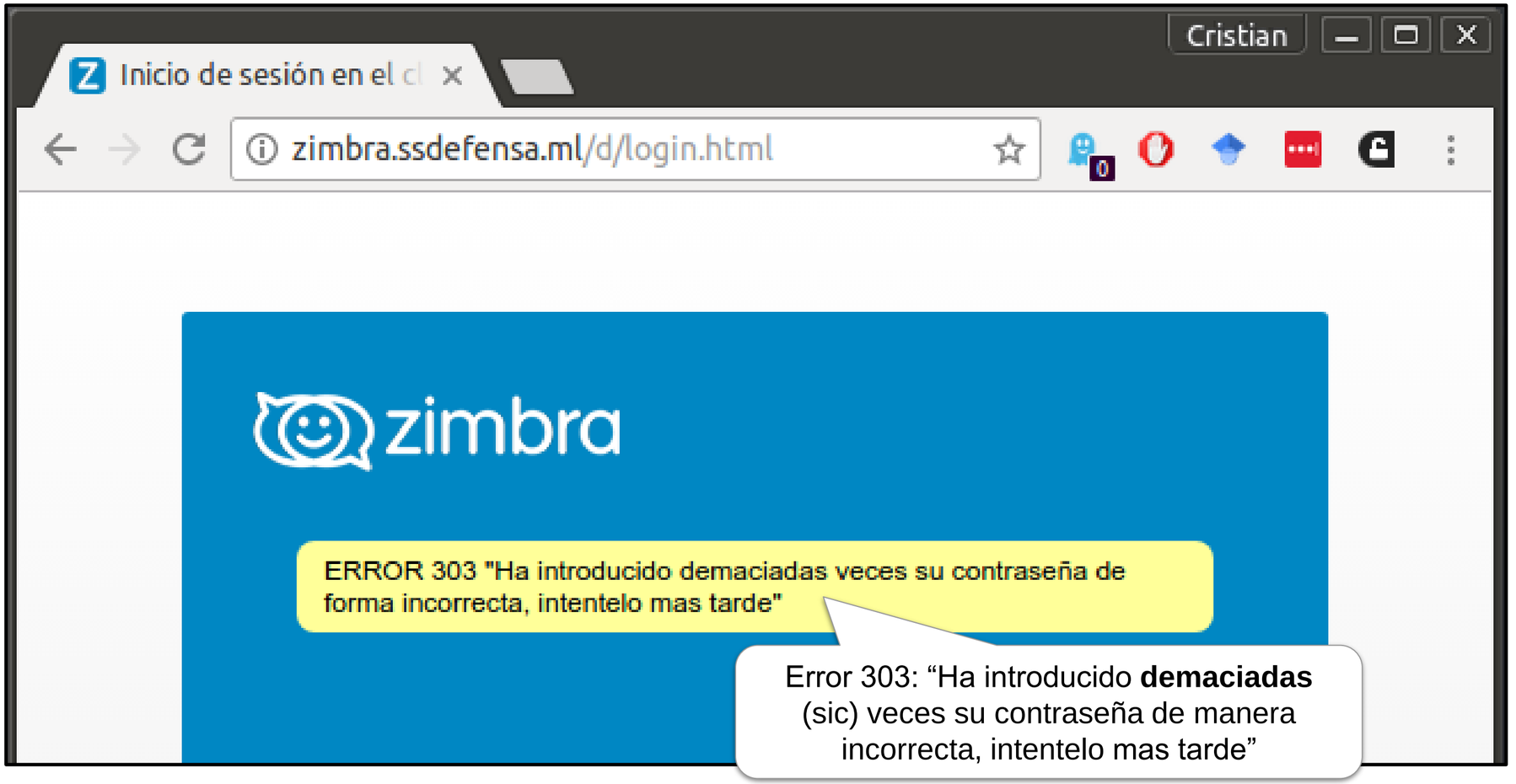
Saludos cordiales, debido a varios intentos de ataques hemos actulizado nuestras politicas de seguridad para la seguridad de todas las cuentas de la Subsecretaria de Defensa, todos los usuarios deben conocer estas politicas de seguridad las cuales se encuentran: AQUI

TAMBIEN ME PERMITO ADJUNTAR MENSAJE MILITAR CON LAS DEBIDAS RECOMENDACIONES SOBRE POSIBLES CORREOS MALICIOSOS.....

ATTE.

Soporte de la Subsecretaria de Defensa

Sitio falsos



Prevención

Cómo protegernos

El mayor riesgo somos nosotros mismos:

- Los ataques exitosos suelen ingresar a equipos y sistemas gracias a que los propios usuarios los autorizan sin querer.

- Capacitar, Capacitar, Capacitar:
    - Si bien las organizaciones cuenta con herramientas tecnológicas (antispam y antivirus) que nos protegen de algunos ataques externos, es de suma importancia entender que la primera barrera de contención somos nosotros mismos.

Para prevenir el phishing

- Desconfiar de cualquier comunicación no solicitada.
  - “Ante la duda, abstente”.
  - Si parece necesario interactuar con el mensaje sospechoso, consultar directamente llamando a la institución o tipeando directamente el sitio oficial en el navegador web.

- Informar a TI de potenciales phishing o actividades extrañas.

- Revisar reglas existentes en nuestros correos, generar acciones de mitigación.

- Tener cuidado con la información que se comparte.
  - Nunca entregar datos confidenciales o autorizar transacciones sin consultarlo con alguien más.

- Mantener estrictos controles manuales sobre operaciones financieras.

Acciones del encargado de ciber contra el malware

- Establecer una política formal que prohíba el uso de software no autorizado.

- Implementar controles que evitan o detectan el uso de software no autorizado (lista blanca) y de controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha son maliciosos (lista negra).

- Establecer una política formal indicando las medidas a tomar para protegerse contra los archivos y software, ya sea de redes externas o a través de cualquier otro medio.

El rol de los trabajadores en la ciberseguridad

- Conocer y respetar las políticas de seguridad de la información
- Considerar todas las descargas como potencialmente inseguras hasta que no sean analizados por una herramienta de detección de malware.
- No ejecutar archivos descargados de servidores externos, de soportes no controlados o adjuntos a correos, sin haber sido previamente analizados.
- Utilizar únicamente el software permitido la institución. Este además debe estar convenientemente actualizado y licenciado [si no es así debe levantar una alerta interna].
- No conectarme a mi equipo con permisos de “administrador”.
- Ante cualquier duda, anomalía o sospecha de anormalidad en su equipo reporte de inmediato al encargado de ciberseguridad.

Sitios falsos

Sitios falsos

Una forma en que los delincuentes buscan acceder a nuestra información, o estafarnos, es a través de sitios falsos.

El envío de links a sitios falsos es común en los ataques de phishing.

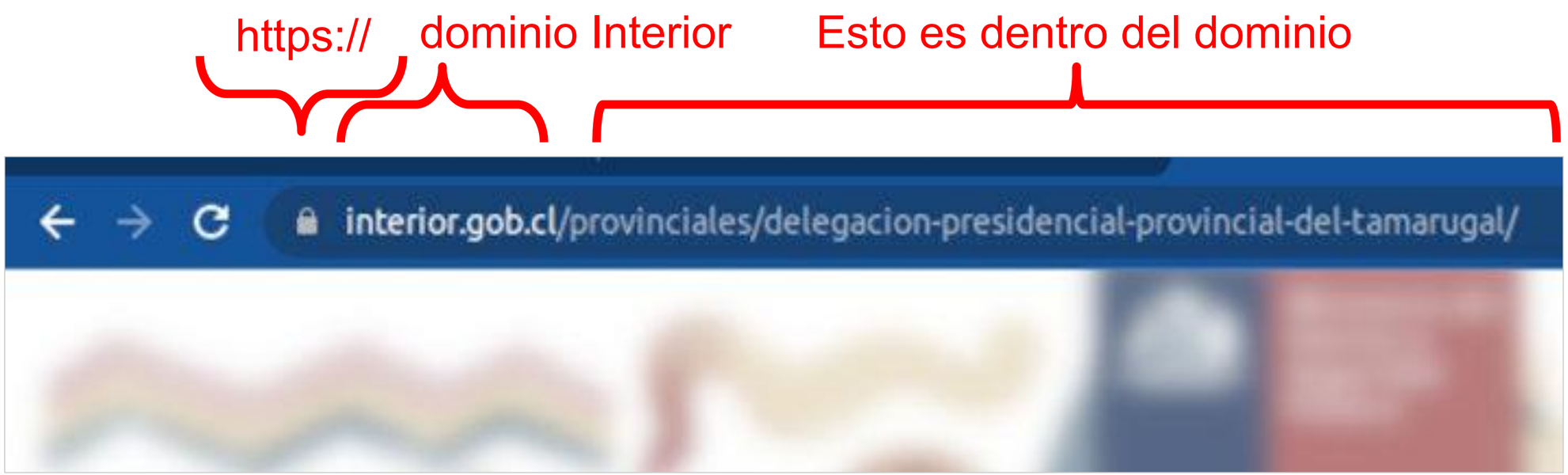
Una página de internet puede verse igual a un sitio legítimo, y ser totalmente falsa. Por eso es clave fijarnos en la URL.

La ortografía también puede ser un indicio. ¡Debemos estar atentos a todos los detalles!

URL

Es una dirección única en el mundo para cada sitio web, documento o lo que sea, en internet. Tiene 4 partes:

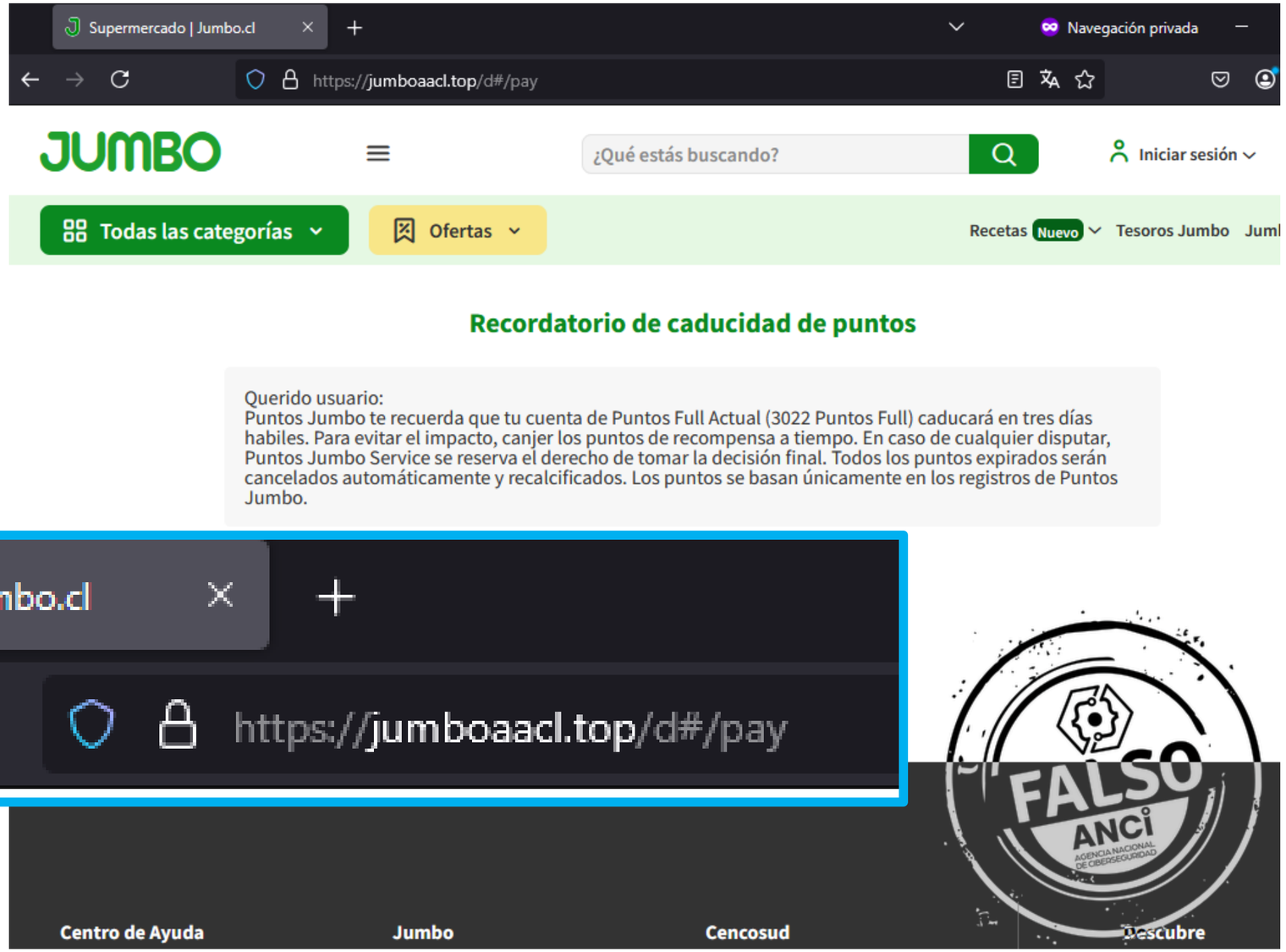
1. **Protocolo**, como http:// o https:// (no siempre se muestra)
2. **Nombre de dominio**. Se lee de derecha a izquierda, y define quién controla el recurso.
3. **Path (ruta)**. Se lee de izquierda a derecha, e indica dónde está el recurso dentro del dominio.
4. **Parámetros**. Una serie de valores que permiten interactuar con el recurso (no siempre presentes).



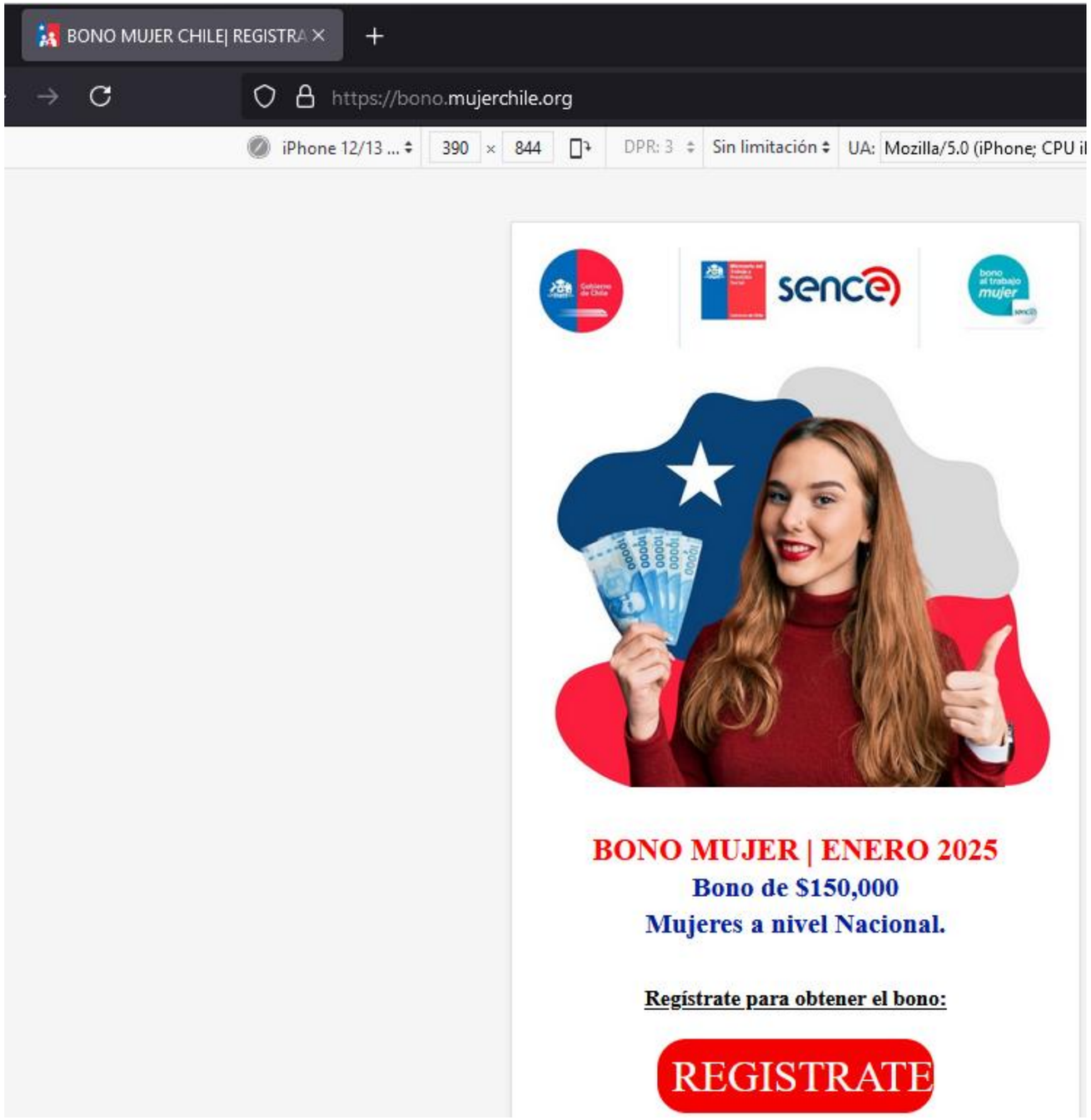
Ejemplos

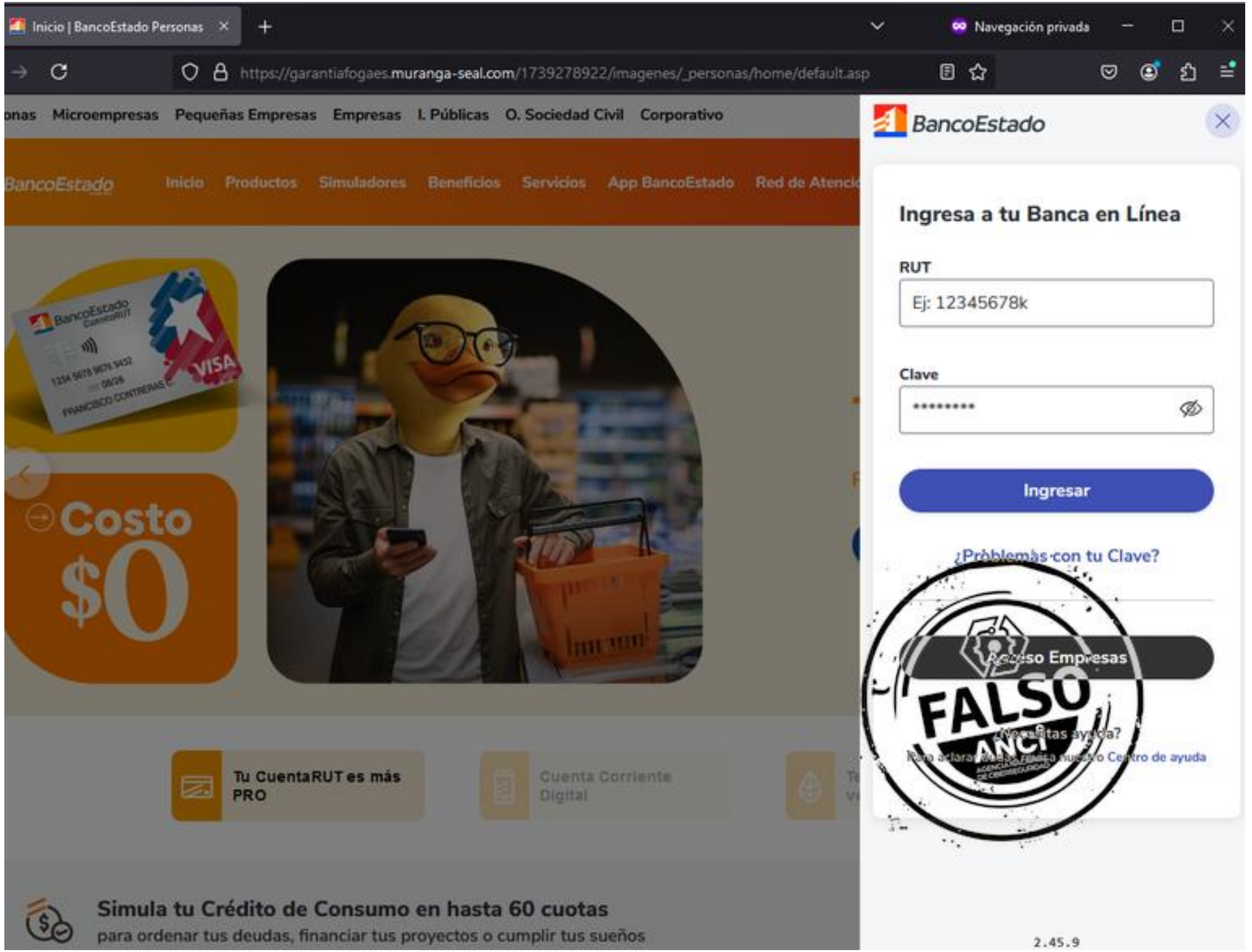

Supermercado | Jumbo.cl
Navegación privada
https://jumboaacl.top/d#/pay
JUMBO
¿Qué estás buscando?
Iniciar sesión
Todas las categorías
Ofertas
Recetas
Nuevo
Tesoros Jumbo
Recordatorio de caducidad de puntos
Querido usuario:
Puntos Jumbo te recuerda que tu cuenta de Puntos Full Actual (3022 Puntos Full) caducará en tres días habiles. Para evitar el impacto, canjer los puntos de recompensa a tiempo. En caso de cualquier disputar, Puntos Jumbo Service se reserva el derecho de tomar la decisión final. Todos los puntos expirados serán cancelados automáticamente y recalcificados. Los puntos se basan únicamente en los registros de Puntos Jumbo.
Próximo Paso
FALSO
ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD
Centro de Ayuda
Jumbo
Cencosud
Descubre

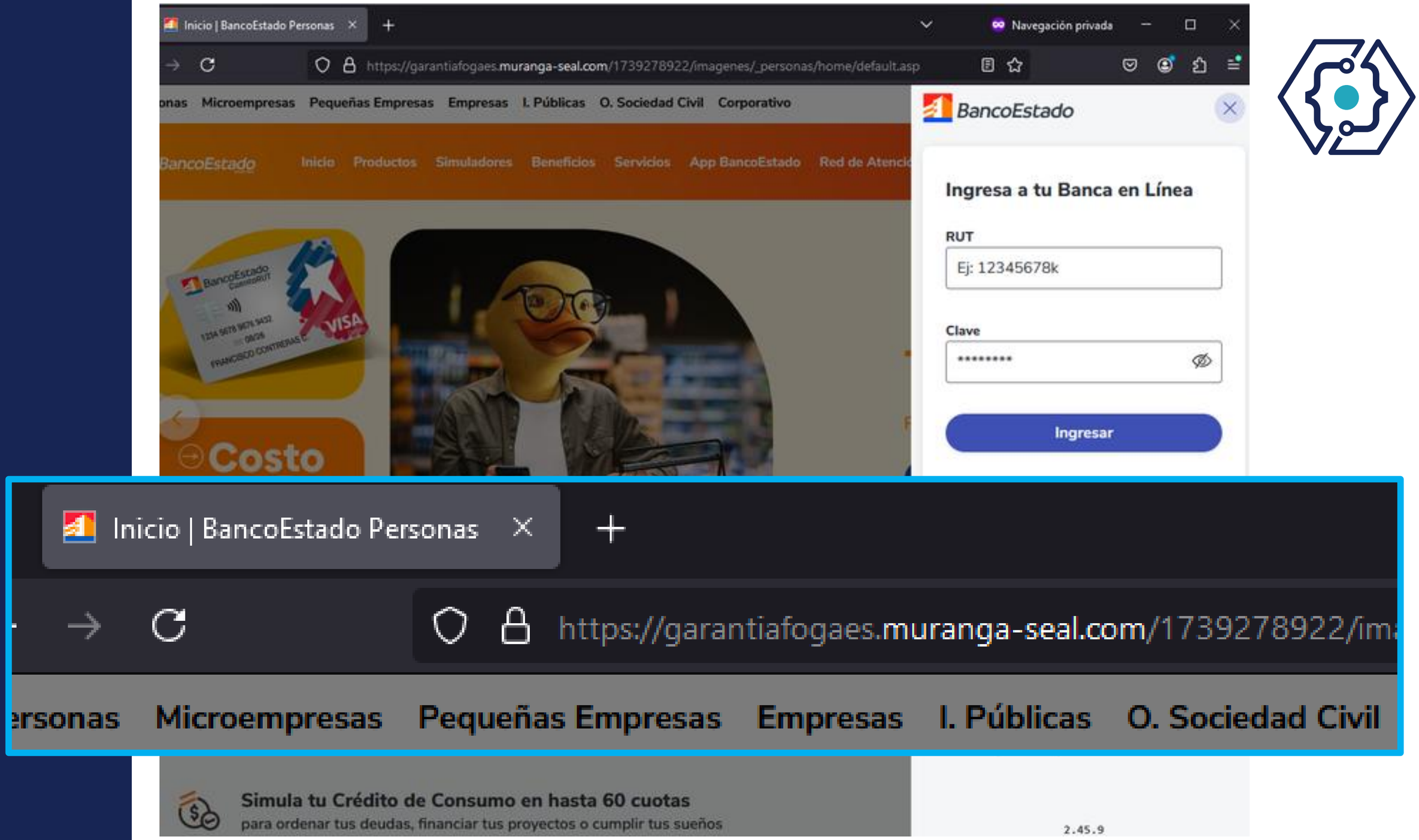
Ejemplos


Supermercado | Jumbo.cl
Navegación privada
https://jumboaacl.top/d#/pay
JUMBO
¿Qué estás buscando?
Iniciar sesión
Todas las categorías
Ofertas
Recetas
Nuevo
Tesoros Jumbo
Recordatorio de caducidad de puntos
Querido usuario:
Puntos Jumbo te recuerda que tu cuenta de Puntos Full Actual (3022 Puntos Full) caducará en tres días habiles. Para evitar el impacto, canjer los puntos de recompensa a tiempo. En caso de cualquier disputar, Puntos Jumbo Service se reserva el derecho de tomar la decisión final. Todos los puntos expirados serán cancelados automáticamente y recalcificados. Los puntos se basan únicamente en los registros de Puntos Jumbo.
Supermercado | Jumbo.cl
https://jumboaacl.top/d#/pay
FALSO
ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD
Centro de Ayuda
Jumbo
Cencosud
Descubre

Ejemplos


BONO MUJER CHILE| REGISTRA
https://bono.mujerchile.org
iPhone 12/13 ...
390
844
DPR: 3
Sin limitación
UA: Mozilla/5.0 (iPhone; CPU il
sence
bono al trabajo mujer
BONO MUJER | ENERO 2025
Bono de $150,000
Mujeres a nivel Nacional.
Regístrate para obtener el bono:
REGISTRATE


Inicio | BancoEstado Personas
Navegación privada
https://garantiafogaes.muranga-seal.com/1739278922/imagenes/_personas/home/default.asp
Microempresas
Pequeñas Empresas
Empresas
I. Públicas
O. Sociedad Civil
Corporativo
Inicio
Productos
Simuladores
Beneficios
Servicios
App BancoEstado
Costo
$0
Tu CuentaRUT es más PRO
Cuenta Corriente Digital
Simula tu Crédito de Consumo en hasta 60 cuotas
para ordenar tus deudas, financiar tus proyectos o cumplir tus sueños
BancoEstado
Ingresa a tu Banca en Línea
RUT
Ej: 12345678k
Clave
Ingresar
¿Problemas con tu Clave?
Acceso Empresas
FALSO
ANCI
¿Necesitas ayuda?
2.45.9


Inicio | BancoEstado Personas
Navegación privada
https://garantiafogaes.muranga-seal.com/1739278922/imagenes/_personas/home/default.asp
Microempresas
Pequeñas Empresas
Empresas
I. Públicas
O. Sociedad Civil
Corporativo
BancoEstado
Inicio
Productos
Simuladores
Beneficios
Servicios
App BancoEstado
Costo
Ingresa a tu Banca en Línea
RUT
Ej: 12345678k
Clave
Ingresar
Simula tu Crédito de Consumo en hasta 60 cuotas
para ordenar tus deudas, financiar tus proyectos o cumplir tus sueños
2.45.9

anci.gob.cl