

Desde Coprom, compartimos información relacionada de **Cinco nuevas campañas de fraude observadas en Chile** recientemente y en estado activo. Revísalas aquí y consejos que presentamos a continuación.

BancoEstado

Se trata de una página web falsa que se hace pasar por Banco Estado para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de la empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Tipo de Alerta

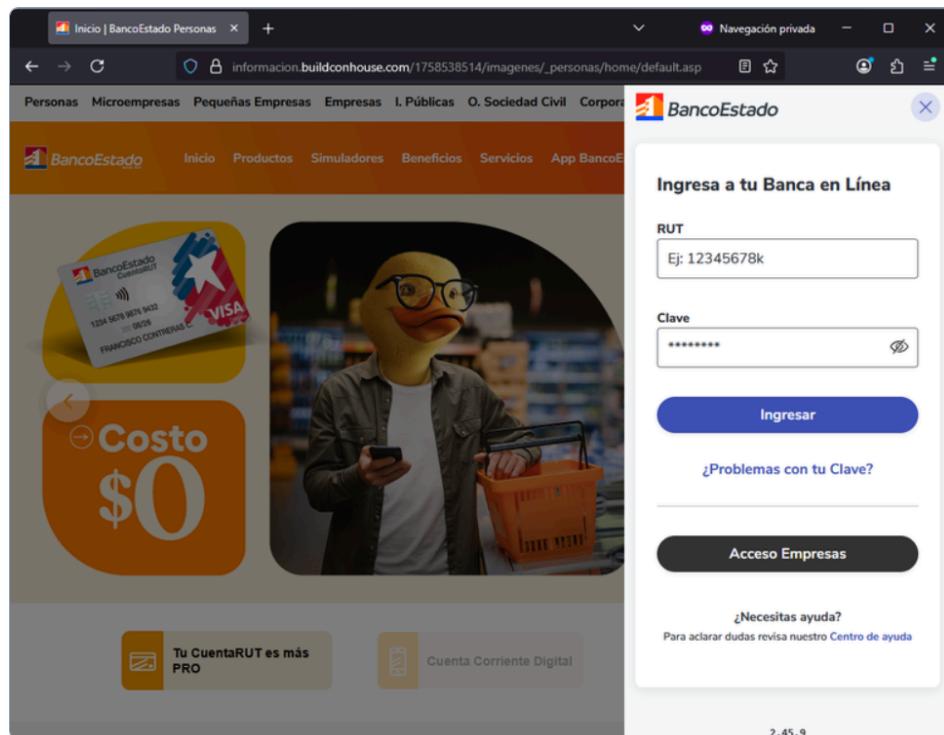
Campaña Fraudulenta

Entidad o aplicación afectada

BancoEstado

Fecha de publicación

22 de septiembre de 2025 a las 09:21



https://informacion.buildconhouse.com/1758538514/imagenes/_personas/home/default.asp

URL sitio falso

Coprec

Se trata de una página web falsa que se hace pasar por Copec para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de esta empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

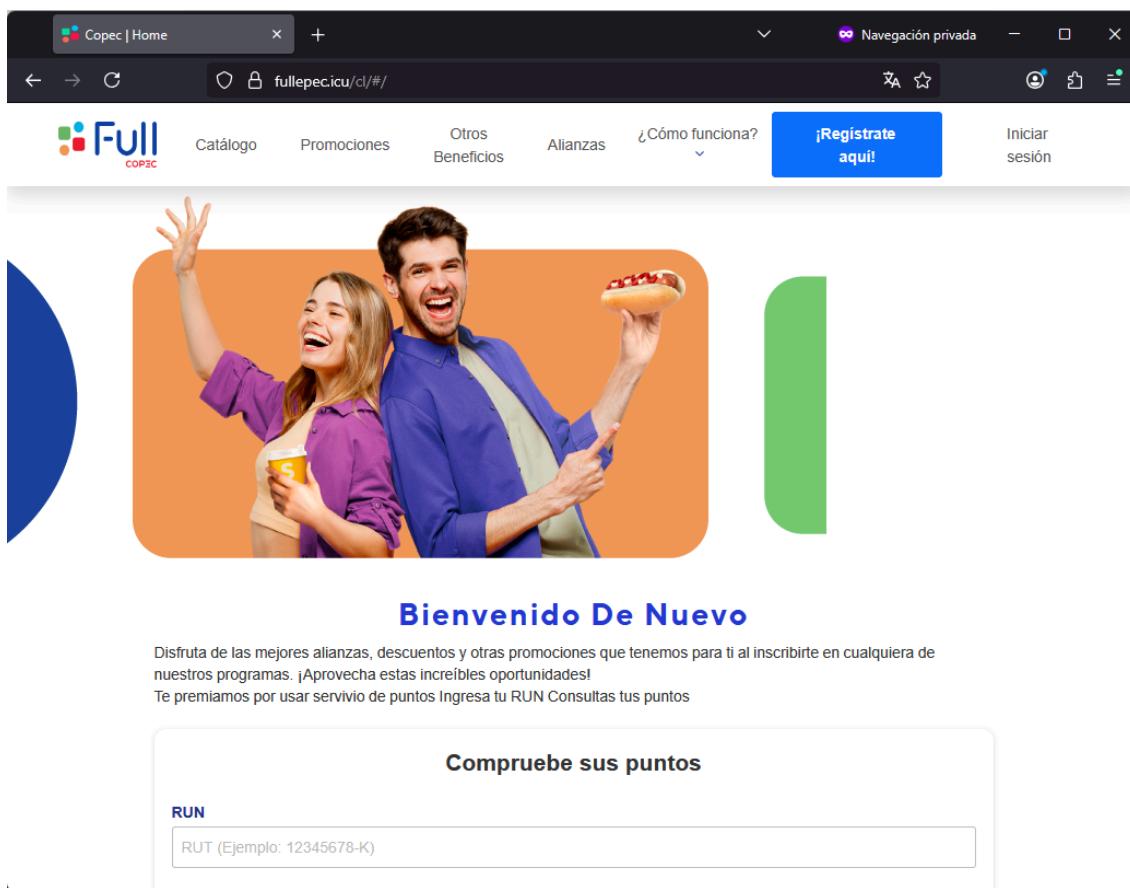
Tipo de Alerta

Campaña Fraudulenta

Entidad o aplicación afectada Coprec

Fecha de publicación

22 de septiembre de 2025 a las 09:21



<https://fullepec.icu/cl/#/>

URL sitio falso

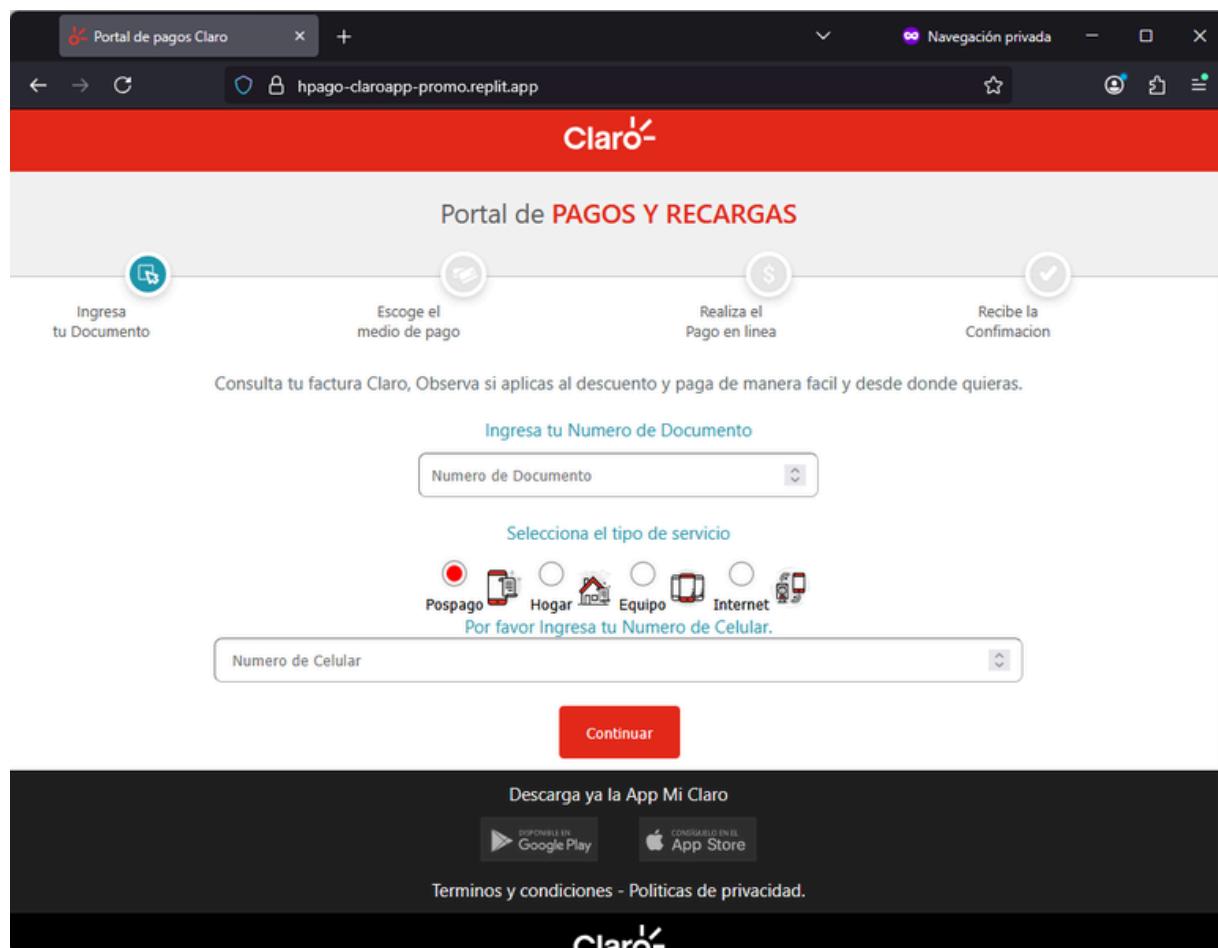
Claro

Se trata de una página web falsa que se hace pasar por Claro para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de Microsoft.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Claro
Fecha de publicación
24 de septiembre de 2025 a las 12:30



The screenshot shows a browser window with the title 'Portal de pagos Claro'. The address bar displays 'hpago-claroapp-promo.replit.app'. The page itself is a仿冒的 Claro payment portal. It features a red header with the 'Claro' logo. Below it, a white section titled 'Portal de PAGOS Y RECARGAS' contains four circular icons representing the steps: 'Ingresa tu Documento', 'Escoge el medio de pago', 'Realiza el Pago en linea', and 'Recibe la Confirmacion'. A message below the icons says 'Consulta tu factura Claro, Observa si aplicas al descuento y paga de manera facil y desde donde quieras.' A form field labeled 'Ingresá tu Número de Documento' is present, along with a dropdown menu for selecting service type. The service type selection area includes radio buttons for 'Pospago' (selected), 'Hogar', 'Equipo', and 'Internet', each accompanied by small icons. A note below the radio buttons says 'Por favor Ingresá tu Número de Celular.' Another input field for 'Número de Celular' is shown. A large red 'Continuar' button is centered at the bottom of this section. Below this, a dark banner promotes the 'Mi Claro' app with download links for Google Play and the App Store. At the very bottom, there are links for 'Términos y condiciones - Políticas de privacidad.' and the Claro logo.

<https://hpago-claroapp-promo.replit.app/>

URL sitio falso

Banco Falabella

Se trata de una página web falsa que se hace pasar por Banco Falabella para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de Microsoft.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Tipo de Alerta

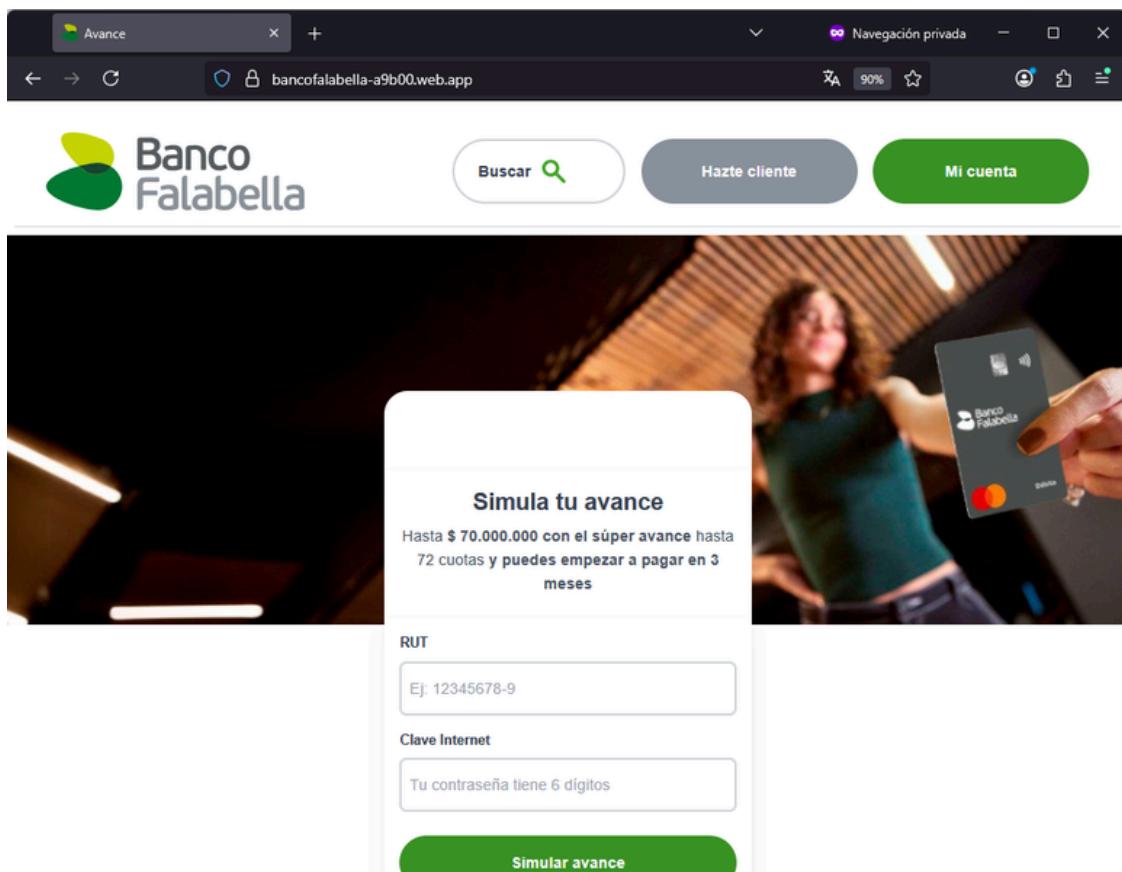
Campaña Fraudulenta

Entidad o aplicación afectada

Banco Falabella

Fecha de publicación

24 de septiembre de 2025 a las
12:32



<https://bancofalabella-a9b00.web.app/>

URL sitio falso

Banco Falabella

Se trata de una página web falsa que se hace pasar por Banco Falabella para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de Microsoft.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Tipo de Alerta

Campaña Fraudulenta

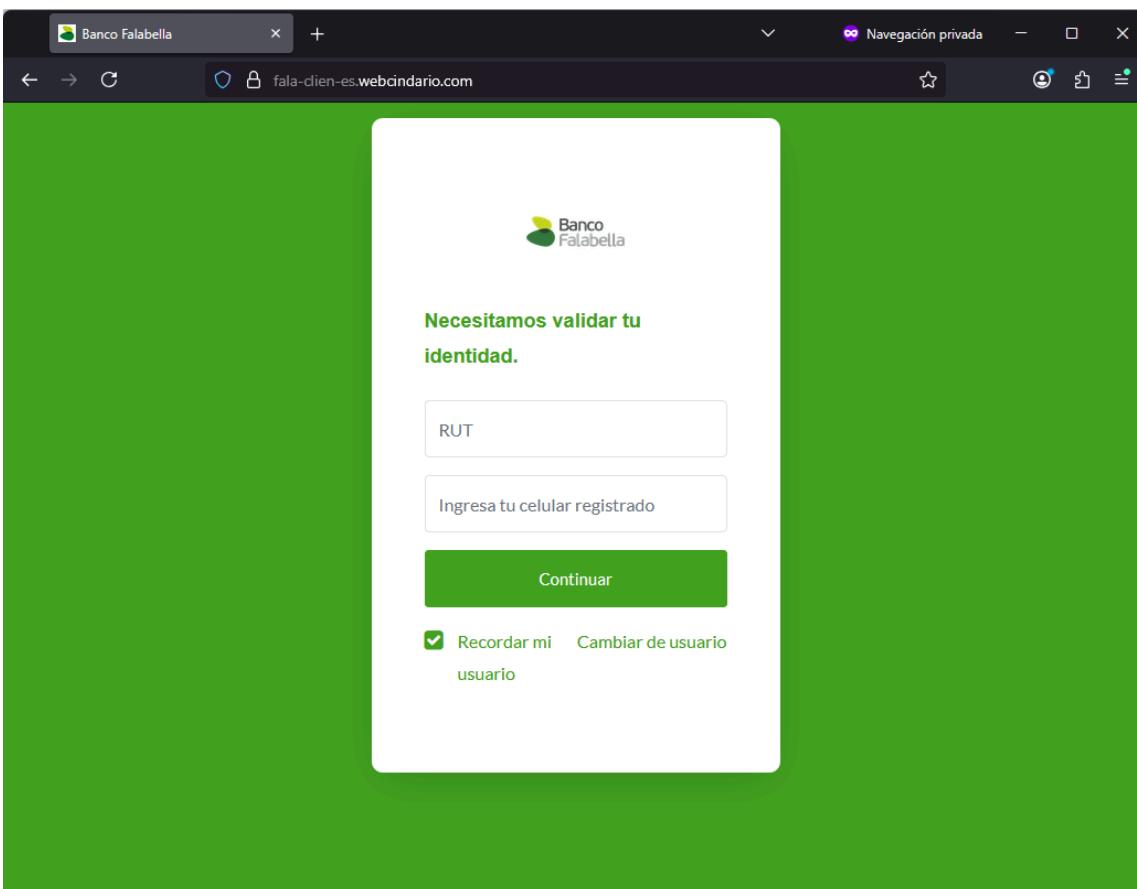
Entidad o aplicación afectada

Banco Falabella

Fecha de publicación

24 de septiembre de 2025 a las

12:32



<https://fala-clien-es.webcindario.com/>

URL sitio falso

Consejos

Semanal	Permanente
<p>Cada vez que tu computador o celular te pida actualizarse, no lo postergues. Más del 60% de los ciberataques exitosos ocurren porque el software estaba desactualizado, ¡aunque ya existía un parche para la falla!</p> <ul style="list-style-type: none">• Actualiza siempre tu sistema operativo, navegador y aplicaciones.• Configura las actualizaciones automáticas cuando sea posible.• Recuerda: actualizar es cerrar la puerta a los delincuentes digitales antes de que entren.	<ol style="list-style-type: none">1. Gestiona tus claves2. Presta atención a las direcciones3. Presta atención a las redes wifi4. Instala las actualizaciones de seguridad de tu computador/teléfono5. Respalda tu información

Últimos Boletines

Revisa aquí los últimos 4 boletines emitidos:

- [Boletín del 23 al 29 de agosto de 2025](#)
- [Boletín del 30 de agosto al 5 de septiembre de 2025](#)
- [Boletín del 6 al 12 de septiembre de 2025](#)
- [Boletín del 13 al 19 de septiembre de 2025](#)