

Revisa las nuevas amenazas y consejos que presentamos a continuación.

## ⚠ Nuevas Amenazas Detectadas

### Tarjeta Bip! - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por la Tarjeta Bip! para robar datos de usuarios, utilizando ilegalmente sus logos e imagen.

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

#### Detalles de la alerta

##### Código

ACF25-00085

##### Tipo de Alerta

Campaña Fraudulenta

##### Entidad o aplicación afectada

Tarjeta Bip!

##### TLP

TLP:CLEAR

##### Fecha de publicación

25 de agosto de 2025 a las 15:57

##### Fecha de última actualización

25 de agosto de 2025 a las 15:57

Actualización de cuenta bip! – Ajuste pendiente



equipo de bip! <mby47i93ds.274736@gmail.com>

Para

[\(i\) Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.](#)

[Responder](#) [Responder a todos](#) [Reenviar](#) [...](#)

dom 24-08-2025 18:39

Estimado/a usuario/a,

Adjuntamos a este correo una factura correspondiente a un pequeño ajuste pendiente en su cuenta bip! por un monto de **\$950 CLP**.

[Factura en PDF](#)

Le agradecemos su atención. Si ya ha realizado el pago, puede ignorar este mensaje.

Atentamente,  
**El equipo de bip!**

[1-click unsubscribe](#)

bip! Servicios de Transporte  
Av. Alameda 1234, Santiago, Chile  
Tel: +56 2 1234 5678 | contacto@tarjetabip.cl

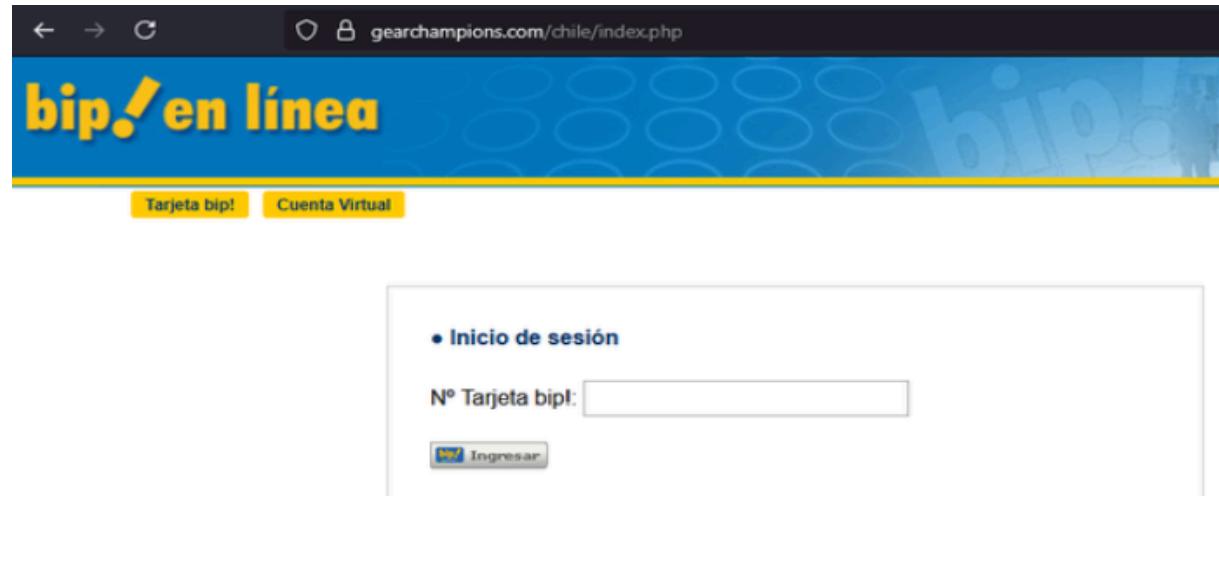
## Factura de Ajuste de Cuenta

Fecha	21 de Agosto de 2025
Número de Factura	INV-20250821-001
Cliente	Usuario de tarjeta bip!
Monto Pendiente	\$950 CLP
Estado	Pendiente de Pago

Gracias por utilizar nuestros servicios. Le recordamos que puede pagar este ajuste en nuestro portal oficial. Si ya ha realizado el pago, no se requiere ninguna acción adicional.

[Hacer Pago Ahora](#)

— bip! Servicios de Transporte



• Inicio de sesión

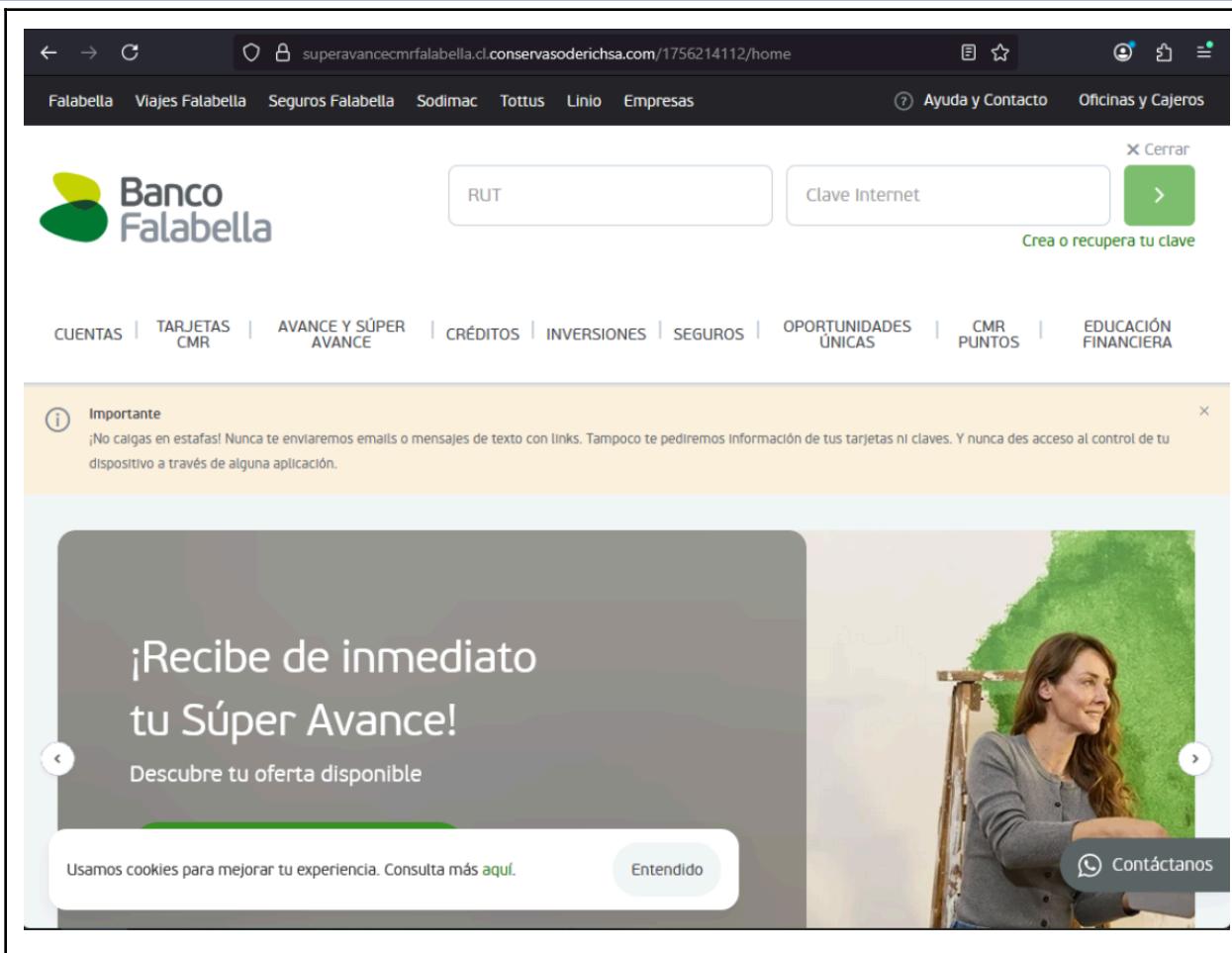
Nº Tarjeta bip!:

 Ingresar

## ANALISIS FORENSE

Valor	Comentario
Actualizaciónde cuenta bip!–Ajuste pendiente	Asunto Email
<a href="https://gearchampions.com/chile/index.php">https://gearchampions.com/chile/index.php</a>	URL sitio falso
<a href="https://go.contactpigeon.com/redir/138626367/78218079/">https://go.contactpigeon.com/redir/138626367/78218079/</a>	URL redirección
<a href="https://mailsrvecom-images.s3.amazonaws.com/private/7Xk32MXn/file1_1756072760%20%281%29.pdf">https://mailsrvecom-images.s3.amazonaws.com/private/7Xk32MXn/file1_1756072760%20%281%29.pdf</a>	Falso documento
<mby47i93ds.274736@gmail.com	Correo de salida

<b>Banco Falabella - Campaña Fraudulenta</b>  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 dicha empresa.  Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.	<b>Detalles de la alerta</b>  <b>Código</b> ACF25-00086 <b>Tipo de Alerta</b> Campaña Fraudulenta <b>Entidad o aplicación afectada</b> Banco Falabella <b>TLP</b> TLP:CLEAR <b>Fecha de publicación</b> 26 de agosto de 2025 a las 12:18 <b>Fecha de última actualización</b> 26 de agosto de 2025 a las 12:18
---	---



The screenshot shows the official website of Banco Falabella ([superavancecmrfalabella.cl.conservasoderichsa.com/1756214112/home](https://superavancecmrfalabella.cl.conservasoderichsa.com/1756214112/home)). The page features the Banco Falabella logo and navigation links for Falabella, Viajes Falabella, Seguros Falabella, Sodimac, Tottus, Lino, Empresas, Ayuda y Contacto, Oficinas y Cajeros, and Cerrar. Below the navigation is a search bar with fields for RUT and Clave Internet, and a button to 'Crea o recupera tu clave'. A horizontal menu includes CUENTAS, TARJETAS CMR, AVANCE Y SÚPER AVANCE, CRÉDITOS, INVERSIONES, SEGUROS, OPORTUNIDADES ÚNICAS, CMR PUNTOS, and EDUCACIÓN FINANCIERA. A prominent banner on the left side of the main content area reads '¡Recibe de inmediato tu Súper Avance!' with a link to 'Descubre tu oferta disponible'. A message at the bottom left states 'Usamos cookies para mejorar tu experiencia. Consulta más [aquí](#)' and a 'Entendido' button. On the right, there is a photo of a woman and a 'Contáctanos' button.

## ANALISIS FORENSE

Valor	Comentario
<a href="https://soscitizens.be/activacion/cuenta-test/">https://soscitizens.be/activacion/cuenta-test/</a>	URL redirección
<a href="https://superavancecmrfalabella.cl.conservasoderichsa.com/1756214112/home">https://superavancecmrfalabella.cl.conservasoderichsa.com/1756214112/home</a>	URL sitio falso

## Lego - Campaña Fraudulenta

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

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

### Detalles de la alerta

**Código**

ACF25-00086

**Tipo de Alerta**

Campaña Fraudulenta

**Entidad o aplicación afectada**

Banco Falabella

**TLP**

TLP:CLEAR

**Fecha de publicación**

26 de agosto de 2025 a las 12:18

**Fecha de última actualización**

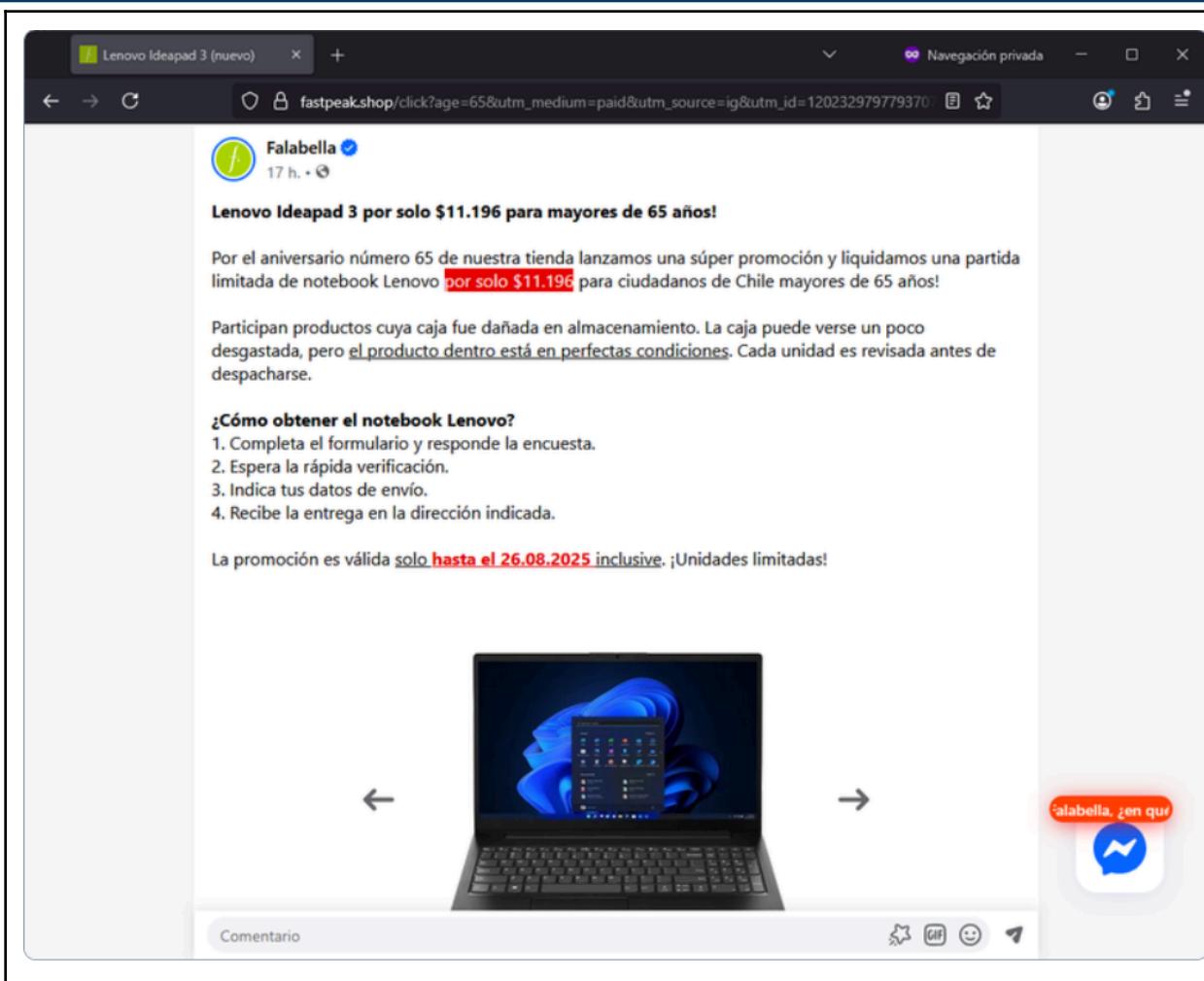
26 de agosto de 2025 a las 12:18



## ANALISIS FORENSE

Valor	Comentario
<a href="https://sellafi.online/">https://sellafi.online/</a>	URL sitio falso

<b>Falabella - Campaña Fraudulenta</b>  <p>Se trata de una página web falsa que se hace pasar por Falabella para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.</p> <p>Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.</p>	<b>Detalles de la alerta</b>  <p><b>Código</b> ACF25-00088</p> <p><b>Tipo de Alerta</b> Campaña Fraudulenta</p> <p><b>Entidad o aplicación afectada</b> Falabella</p> <p><b>TLP</b> TLP:CLEAR</p> <p><b>Fecha de publicación</b> 26 de agosto de 2025 a las 12:18</p> <p><b>Fecha de última actualización</b> 26 de agosto de 2025 a las 12:18</p>
--	--



The screenshot shows a Facebook post from Falabella. The post features a headline: "Lenovo Ideapad 3 por solo \$11.196 para mayores de 65 años!". It includes a message: "Por el aniversario número 65 de nuestra tienda lanzamos una súper promoción y liquidamos una partida limitada de notebook Lenovo **por solo \$11.196** para ciudadanos de Chile mayores de 65 años!" Below this, there's a note about the condition of the products and a list of steps to obtain the notebook. The post ends with a note that it's valid until August 26, 2025. A photo of a black Lenovo Ideapad 3 laptop is displayed, showing its screen and keyboard. A red button on the right says "Alibaba, ¿en qué?".

## ANALISIS FORENSE

Valor	Comentario
<a href="https://fastpeak.shop/">https://fastpeak.shop/</a>	URL sitio falso

## Microsoft - Campaña Fraudulenta

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

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

### Detalles de la alerta

**Código**

ACF25-00089

**Tipo de Alerta**

Campaña Fraudulenta

**Entidad o aplicación afectada**

Microsoft

**TLP**

TLP:CLEAR

**Fecha de publicación**

26 de agosto de 2025 a las 12:17

**Fecha de última actualización**

26 de agosto de 2025 a las 12:17

Important!: We Couldn't Process Your Microsoft Subscription Renewal, Mon, 25 Aug 2...



Microsoft Billing Failure &lt;sl&gt;

 Aceptar Provisional No aceptar

...

lun 25-08-2025 13:33

Necesario

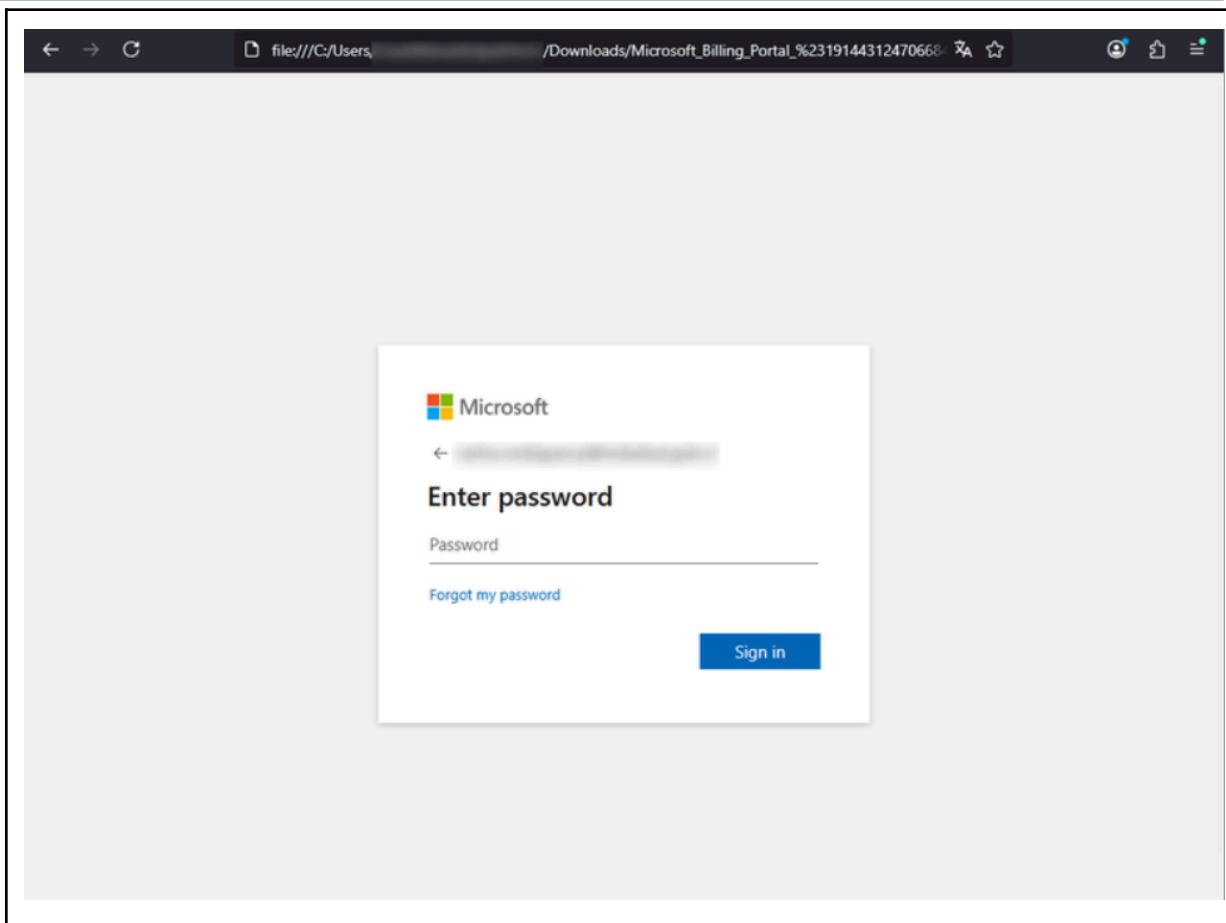
Opcional

(i) Como organizador de la reunión, no tiene que responder a la reunión.



Microsoft\_Billing\_Portal\_#191443124706684586.htm

12 KB



## ANALISIS FORENSE

Valor	Comentario
https://nhpfggop.emeluxewigs.co.za:8443/impact?cid8R7KWD8G={Correoelectronico}	URL sitio falso
Important ! :WeCouldn'tProcessYourMicrosoftSubscriptionRenewal,Mon,25Aug202510:33:19-0700	Asunto Email
mmoraoseguera@support.captainhomes.ca	Correo de salida

## Microsoft - Campaña Fraudulenta

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

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

### Detalles de la alerta

<b>Código</b>	ACF25-00090
<b>Tipo de Alerta</b>	Campaña Fraudulenta
<b>Entidad o aplicación afectada</b>	Microsoft
<b>TLP</b>	TLP:CLEAR
<b>Fecha de publicación</b>	29 de agosto de 2025 a las 08:38
<b>Fecha de última actualización</b>	29 de agosto de 2025 a las 08:38

SOA For Your Review id:535b19e268df9f54f46ecaede5cbeb6f1d6a3cd1



Adobe Document Services-535b19e268df9f54f46ecaede5cbeb6f1d6  
Para

Responder Responder a todos Reenviar ...

jue 21-08-2025 13:58

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

### Adobe Sign

#### Document Delivered

Hello Malbagli,

A document has been shared with you via Adobe Sign. Please review the details below and sign it at your earliest convenience so we can process payment.:.

- **Document Name:** Statement Of Account & Past due Invoices.xlsx.
- **Document Name:** Savalcorp\_Authorized-Signers\_Review.docx.
- **Delivered on:** August 21, 2025 at 5:58:07 PM UTC.

[Review Document](#)

© 2025 Microsoft Corporation. One Microsoft Way, Redmond, WA 98052  
You received this email because you're an active Microsoft Office user.

## ANALISIS FORENSE

Valor	Comentario
eronsman@palmwineboys.com	Correo de salida
<a href="https://agrutrou.stebugea.sa.com/jc@M2CG3c4rLB/\${Correoelectrónico}">https://agrutrou.stebugea.sa.com/jc@M2CG3c4rLB/\${Correoelectrónico}</a>	URL redirección
<a href="https://agrutrou.stebugea.sa.com/k5af3grrsq11?id=80cec29857dfbbd98-972bd2c1e64246-12cd2980ec9b8-0c1cf6bd471-67773fdcb8-4e563c6a04-3dab0c74d389b-068da64ec15b09c88aaca4">https://agrutrou.stebugea.sa.com/k5af3grrsq11?id=80cec29857dfbbd98-972bd2c1e64246-12cd2980ec9b8-0c1cf6bd471-67773fdcb8-4e563c6a04-3dab0c74d389b-068da64ec15b09c88aaca4</a>	URL sitio falso
<a href="https://t.yesware.com/tt/2502560518384679c184679604337623c9594452/a98278710594448804543c809c846794/9488045f35e5944e594404aa60433762/abralliance.com/{Correoelectronico}">https://t.yesware.com/tt/2502560518384679c184679604337623c9594452/a98278710594448804543c809c846794/9488045f35e5944e594404aa60433762/abralliance.com/{Correoelectronico}</a>	URL redirección



SOAForYourReviewid:535b19e268df9f54f46ecaede5cbeb6f1d6a3cd1

Asunto email



## Consejos

Semanal	Permanente
No prestes tu celular desbloqueado. Muchas apps quedan abiertas y alguien puede enviarse información sensible en segundos.	<ol style="list-style-type: none"><li>1. Gestiona tus claves</li><li>2. Presta atención a las direcciones</li><li>3. Presta atención a las redes wifi</li><li>4. Instala las actualizaciones de seguridad de tu computador/teléfono</li><li>5. Respalda tu información</li></ol>