



Fraudes bancarios: ¡Evita caer en el phishing!

El **phishing** es un método de ingeniería social que usa correos electrónicos, SMS, WhatsApp, llamadas o sitios web falsos para **obtener información confidencial** a través de enlaces con software malicioso.



¿Cómo evitar el phishing?



1 Sé escéptico ante los correos y mensajes sospechosos



- No hagas clic a cualquier enlace o archivo.
- Chequea antes la **legitimidad del remitente**.

2 Verifica la URL de los sitios web



- Los sitios seguros comienzan con "**https://**".
- Muestran un **candado** en la barra de direcciones.

3 Corroboras cualquier solicitud de información con tu banco



- **Nunca entregues contraseñas**, números de tarjetas u otra información.
- Verifica llamando **directamente a tu banco**.

4 Utiliza la autenticación de dos factores (2FA)



- Agrega una **nueva capa de seguridad** a tus cuentas.
- Este mecanismo **exige cada vez un código temporal** para ingresar.

5 Revisa y actualiza tus cuentas periódicamente



- **Verifica regularmente** tus transacciones y renueva contraseñas de forma periódica.
- Ante alguna **acción desconocida**, llama a tu banco.



En caso de fraudes

Bloquea cuentas y tarjetas, realiza aclaraciones con el banco y denuncia en el **Portal de Fraudes Financieros** de la **CONDUSEF**.

