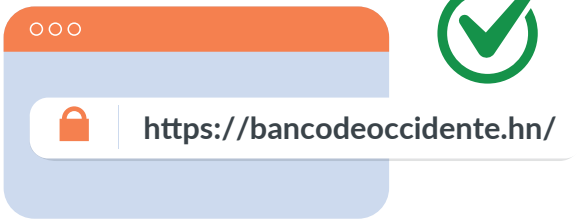
¡Juntos contra el fraude!

¿Cómo detectar una dirección web falsa?

- **Errores ortográficos**
- **Palabras extras**

La dirección web correcta es



Banco de Occidente S.A NUNCA solicitará a través de llamadas, correos electrónicos, mensajes de texto o WhatsApp información de cuentas o canales electrónicos.

Si has sido víctima de un intento de fraude llama al:
2290-7000 o 2545-7000

Nuestros canales oficiales son:

- *www.bancodeoccidente.hn*
- *@bancocci*
- *@bancodeoccidente*
- *@bancocci*
- *Banco de occidente S.A. Honduras*
- *2290-7000*

¡Protejamos tu futuro!

Conoce más

¡Juntos contra el fraude!

Asegura tus ahorros

¡Protejamos tu futuro!

Banco de Occidente

El fraude se puede prevenir

No se deje engañar, aquí le presentamos los tipos de fraudes que existen y algunos consejos para evitarlos.

1- ¿Qué son los fraudes financieros?

Son acciones que una persona realiza con el fin de obtener un beneficio propio a costa de dañar la economía de otra persona.

La mayoría de los defraudadores buscan conseguir tus datos para sacar un beneficio económico ilícito.

2- Tipos de fraudes financieros

- Sorteos falsos con depósitos para reclamar el premio.

- Falsas ofertas de empleo solicitando depósito por reclutamiento

- Paquetería inesperada solicitando datos personales y depósito para pago de impuestos.

- Fraudes cibernéticos:

- **PHISHING:** Es la suplantación de identidad de una compañía u organismos públicos que a través de enlaces o sitios webs fraudulentos solicitan información personal y bancaria.

- **ANGLER PHISHING:** A través de perfiles falsos en redes sociales, los delincuentes pueden robar tu información.

- **SMISHING:** Son robos que se cometen por medio de mensajes de texto o chats simulando ser entidad legítima del banco.

- **VISHING:** Son estafas por teléfono en las que un delincuente se hace pasar por empleado de algún banco para obtener información.

- **SIM Swapping:** Consiste en obtener un duplicado o clon de una tarjeta SIM, para suplantar la identidad del titular de la línea y poder acceder a sus cuentas bancarias a través del envío de un mensaje SMS (código OTP) utilizado como doble factor de autenticación.

3- ¿Cómo evitar ser víctima de fraude?

- Verifica si la dirección Web es correcta

- Escribe desde tu buscador el sitio oficial del banco.

- Evite iniciar sesión de la cuenta bancaria a través de correos electrónicos sospechosos, o, Whatsapps.

- Nunca entregue un anticipo para obtener un beneficio (premio, trabajo, producto entre otros)

- No compartas tu información de cuentas, códigos de seguridad o datos personales con ninguna institución mediante llamadas telefónicas, mensajes de texto o correos dudosos sin importar su origen.

- Asegúrese de verificar el enlace a la página web oficial de Banco de Occidente S.A

https://bancodeoccidente.hn/

- Crear sus contraseñas más robustas las cuales pueden contener letras, números y símbolos.