Anatomía de un anuncio **FALSO** en Facebook

¡Es un intento de fraude!



1. El nombre es de una página personal
2. Las condiciones son irregulares
3. El enlace no es el de la página web oficial del banco o es un enlace sospechoso.

Recuerda, **NUNCA** te solicitaremos renovar tus datos personales,token, código OTP, usuario ni contraseñas a través de correo electrónico,llamadas telefónicas o mensajes de texto.

Juntos contra el fraude

¡Juntos contra el fraude!

Banco de Occidente 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

Banco de Occidente | 75 ANIVERSARIO

Contact Center
2545-7000/2290-7000

WhatsApp:
9470-7000

Banco de Occidente Honduras

www.bancodeoccidente.hn

Asegura tus ahorros

Banco de Occidente | finanzas con Voz

Conoce sobre el fraude



finanzas con Voz

El fraude se puede prevenir

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

Qué son los fraudes financieros?

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

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

Tipos 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 organismos públicos que a través de enlaces o sitios web fraudulentos solicitan información personal y bancaria.

ANGLER PHISHING: Es una estafa en redes sociales donde delincuentes suplantan cuentas de atención al cliente de empresas legítimas para robar datos.

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.

¿cómo evitar ser víctima de fraude?

Verifica si la dirección Web es correcta.

Escribe desde tu buscador el sitio oficial del banco.

NO iniciar sesión de tus canales electrónicos a través de correos electrónicos sospechosos, WhatsApp, redes sociales.

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

NO compartas información de tus cuentas, códigos de seguridad o datos personales a través de llamadas, mensajes de texto o correos sospechosos, sin importar su origen.

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

https://bancodeoccidente.hn/

Identifique una dirección de web falsa revisando errores ortográficos, palabras adicionales o diferencias con el sitio oficial de la entidad.