NO SEAS VÍCTIMA DE

FRAUDE POR TRANSFERENCIA

1845 TITLE

La información sensible desempeña un papel crítico en tu transacción inmobiliaria, y es imprescindible que esta información se mantenga segura y protegida.

Los estafadores aprovechan cada vez más a los compradores de vivienda durante el proceso de cierre, utilizando una técnica conocida como phishing o suplantación de identidad. Durante una transacción inmobiliaria, intentan desviar los costos de cierre y el pago inicial de un comprador a una cuenta fraudulenta, haciéndose pasar por un representante de la compañía de títulos, el prestamista o el agente inmobiliario. Por ejemplo, podrían enviar un correo indicando que ha habido un cambio de último minuto en las instrucciones de transferencia y solicitar que los fondos se envíen a la nueva cuenta provista. Al seguir estas instrucciones, los fondos se transfieren inadvertidamente a la cuenta del estafador y, en la mayoría de los casos, se pierden para siempre. Como consumidor, existen formas de identificar y protegerte contra el cibercrimen.

DETENTE. LLAMA. VERIFICA.

SOLICITUDES URGENTES

Ten cuidado con correos que solicitan cambios de último minuto en las instrucciones de transferencia, imponen un plazo estricto para realizar una acción o son de tono amenazante.

DIRECCIÓN DEL REMITENTE

Confirma que la dirección de correo electrónico del remitente coincide con el nombre y la dirección de respuesta. Estas direcciones falsas parecen legítimas, pero suelen tener una letra adicional o alguna variación menor respecto a la dirección real.

ARCHIVOS ADJUNTOS Y ENLACES

Evita hacer clic en enlaces o descargar archivos adjuntos que puedan instalar archivos maliciosos en tu computadora, sin antes confirmar con tu representante de confianza.

FALTAS DE ORTOGRAFÍA O GRAMÁTICA DEFICIENTE

Los mensajes de phishing suelen contener palabras mal escritas o errores gramaticales.

SALUDO IMPERSONAL

Los correos de phishing pueden utilizar saludos genéricos como: “Hola estimado” o “Cliente Valorado”.

FIRMA DEL CORREO ELECTRÓNICO

Verifica si el cierre del correo es demasiado genérico o no coincide con la plantilla oficial de la empresa.

QUÉ HACER SI HAS SIDO VÍCTIMA

Si tienes alguna duda, llama directamente a tu representante para confirmar cualquier cambio. Utiliza un número de teléfono que esté públicamente disponible, o uno que te haya sido proporcionado directamente por el representante, no el número incluido en el correo electrónico. Aunque pueda parecer que nunca caerías en este tipo de estafa, los esquemas son complejos y muchas veces parecen legítimos. Si sospechas que has sido víctima de fraude por transferencia bancaria, contacta inmediatamente con tu banco o la empresa de transferencias. Solicita una revocación de la transferencia. Reportar el error lo antes posible puede aumentar la probabilidad de que recuperes tu dinero.