Fraudes en el sector inmobiliario: verifique antes de pagar

By Jeff Ostrowski

Los compradores de viviendas están siendo víctimas de fraudes electrónicos en el sector inmobiliario, en parte debido a la falta de seguridad cibernética y al complicado proceso de venta. Muchos nunca recuperan su dinero.

Tim Myers estaba a punto de cerrar la compra de una casa en Fort Wayne, Indiana, cuando el correo electrónico que estaba esperando apareció en su bandeja de entrada. Su agente de préstamos hipotecarios envió instrucciones para la transferencia bancaria de su pago inicial, junto con una solicitud para enviar el dinero en las próximas horas. Myers y su esposa fueron a su sucursal de Flagstar y transfirieron $34,000 a una cuenta del Bank of America.

Todo parecía estar bien, hasta el día siguiente, cuando la compañía de títulos que manejaba el cierre envió instrucciones para transferir el pago inicial a través de un portal seguro. Myers llamó a la compañía para decir que ya había enviado el dinero.

Luego llegó la terrible noticia: lo habían estafado.

Afortunadamente, Myers pudo cerrar la compra de la propiedad de todos modos y finalmente recuperó el dinero robado. En muchos casos, las víctimas de fraude de depósito en garantía de bienes raíces nunca vuelven a ver su dinero en efectivo, según FinCEN, el brazo de cumplimiento del Departamento del Tesoro de los EE. UU.

Cómo funciona el fraude de depósito en garantía

El FBI clasifica el fraude de depósito en garantía como "correo electrónico comercial comprometido". En 2023 se denunciaron más de 21.000 delitos de este tipo, con pérdidas totales de casi 3.000 millones de dólares ese año.

Las cantidades robadas pueden ser devastadoras. En un ejemplo, el FBI informa que ayudó a una víctima a recuperar 426,000 dólares transferidos por una casa en Stamford, Connecticut, en 2023. Los estafadores saben que en las transacciones inmobiliarias se mueve mucho dinero. En el momento del cierre, el comprador presenta un pago inicial o

incluso el importe total de la compra al vendedor, una suma de decenas o cientos de miles.

Con todo ese dinero en garantía en juego, los estafadores buscan un vínculo de ciberseguridad débil en algún lugar de la transacción, normalmente afiliado al agente inmobiliario, el oficial de préstamos, la compañía de títulos o el abogado de cierre.

Luego comienza el hackeo. Una vez que los estafadores obtienen acceso a la actividad en línea de esa persona o entidad, se enteran de quién está a punto de comprar una casa. El comprador recibe un correo electrónico, una llamada telefónica o un mensaje de texto de alguien que dice ser el abogado de liquidación o la compañía de títulos con instrucciones sobre dónde transferir los fondos.

Eso es lo que le pasó a Myers. El correo electrónico que recibió incluía una descripción precisa de la propiedad que estaba comprando, un logotipo de la empresa y la información de contacto del oficial de préstamos.

"Parecía legítimo", dice Myers. "Incluso tenía las instrucciones de 'Cuidado con el fraude electrónico'".

Señales de fraude electrónico inmobiliario

El correo electrónico no coincide exactamente. Los estafadores suelen utilizar direcciones de Gmail en lugar de

direcciones afiliadas a un dominio de la empresa. En un caso, la dirección de correo electrónico inicial puede parecer legítima, pero si pulsa responder, verá una dirección diferente para el destinatario.

Las instrucciones de transferencia bancaria se encuentran en el cuerpo del correo electrónico, en lugar de en un portal seguro.

El correo electrónico parece urgente o confuso. El estafador puede insistir en que la transferencia bancaria debe realizarse de inmediato, o las instrucciones pueden contradecir lo que su agente de cierre le dijo que sucedería.

El correo electrónico contiene un formato, una gramática o una ortografía extraños. Si el correo electrónico fuera de hecho de su agente de préstamos hipotecarios o compañía de títulos, estaría escrito de manera profesional, sin espacios ni palabras extrañas.

El estafador no atenderá llamadas telefónicas. Incluso si el correo electrónico contiene un número de teléfono, el estafador puede afirmar que está demasiado ocupado para responder.

Está realizando un pago inicial significativo. Los estafadores tienen más probabilidades de centrarse en transacciones que implican grandes pagos iniciales y menos probabilidades de buscar préstamos con un pago inicial nulo o muy bajo.

Por lo general, los estafadores trasladan el dinero de una cuenta bancaria a otra. Desde allí, el dinero suele trasladarse al extranjero o a criptomonedas, donde es prácticamente imposible rastrearlo e recuperarlo, dice Claudia Lee, vicepresidenta de CertifID, una empresa que ofrece servicios de recuperación de fraudes y vende seguros contra fraudes electrónicos.

"Somos muy realistas en cuanto a que si han pasado más de 24 a 48 horas, las posibilidades de recuperación no son grandes, aunque tampoco eran buenas para empezar", dice Lee.

Myers había transferido los 34.000 dólares a la hora del almuerzo un lunes y se dio cuenta de que lo habían estafado al mediodía del martes. Decidió que había enviado el dinero a una sucursal del Bank of America en Indianápolis. Después de numerosas llamadas telefónicas, se puso en contacto con un gerente de sucursal que accedió a marcar la transacción para un examen más detallado.

Los delincuentes habían sido frustrados, por poco.

"Tuvieron aproximadamente 24 horas para hacer lo que querían y, afortunadamente, yo fui más rápido que ellos", dice Myers.

Myers denunció el delito a las autoridades locales, estatales y federales y se puso en contacto con CertifID. Después de unos cuatro meses de llamadas telefónicas estresantes, le devolvieron el dinero.

Myers tuvo suerte. Solo el 22 % de las 2000 víctimas de fraude de depósito en garantía que presentaron denuncias en 2020 y 2021 recuperaron todo su dinero, según Fin-CEN.

A pesar del resultado favorable, el crimen persiguió las finanzas de Myers durante meses. Debido a que su cuenta corriente de Flagstar había sido comprometida, se vio obligado a congelar la actividad. Eso provocó que no se enviaran pagos automáticos, como uno a la guardería de sus hijos.

Myers todavía no tiene idea de quién estaba detrás del intento de robo.

"Fue una larga experiencia", dice Myers. "Fue un dolor de cabeza, por decir lo menos".

Tome este paso adicional

El fraude electrónico ha ganado popularidad entre los delincuentes por varias razones. En parte se debe a que las ventas de viviendas están dirigidas por un ecosistema en expansión con muchas formas en que los estafadores pueden colarse y muchos actores que podrían no ejercer una

vigilancia constante en torno a la ciberseguridad. La Asociación Nacional de Agentes Inmobiliarios® tiene 1,5 millones de miembros, casi todos ellos contratistas independientes. La Asociación Estadounidense de Títulos de Propiedad cuenta con 6.000 miembros, muchos de ellos pequeñas empresas de títulos. Más de 5.000 prestamistas originaron hipotecas en los EE. UU. en 2023, según datos federales.

El objetivo final es el comprador de la vivienda, muchos de ellos en una larga y complicada venta llena de pasos aparentemente interminables y una jerga desconcertante.

"Es un proceso abrumador, especialmente para quienes compran por primera vez", dice Diane Tomb, directora ejecutiva de la Asociación Estadounidense de Títulos de Propiedad, que aconseja a los compradores tomar la rápida decisión de levantar el teléfono para verificar las instrucciones antes de ejecutar una transferencia bancaria.

"Parece simple, pero no lo es cuando estás en medio de todo", dice Tomb.

En retrospectiva, Myers se dio cuenta de que debería haber sido más cauteloso. Si bien el correo electrónico con las instrucciones de la transferencia bancaria mostraba el nombre de su agente de préstamos, al inspeccionarlo más a fondo resultó que provenía de una cuenta de Gmail en lugar del dominio de la compañía hipotecaria. El destinatario de la

transferencia bancaria no era una empresa, sino un individuo, otra señal de alerta.

Ninguno de esos signos era lo suficientemente obvio como para despertar las sospechas de Myers. Lee, de CertifID, dice que los estafadores han pulido el esquema para que solo los compradores de viviendas más paranoicos noten las imperfecciones.

"Son buenos en eso", dice Lee. "Hacen que parezca y suene muy creíble. Y se aprovechan del hecho de que la transferencia bancaria es urgente. Nadie quiere perder la casa".

Myers también experimentó de primera mano las lagunas en las protecciones al consumidor. Los bancos reembolsan rutinariamente a los clientes por transacciones no autorizadas, como retiros fraudulentos o cargos falsos en tarjetas de crédito. Dado que Myers había autorizado la transferencia bancaria al estafador, esas protecciones no se aplicaban.

En el caso de Myers, la respuesta de las fuerzas del orden tampoco fue muy tranquilizadora. Habló con un agente del FBI, pero la naturaleza transjurisdiccional del delito complica las investigaciones, al igual que la falta de un autor fácilmente identificable.

Myers cree que aprendió una valiosa lección: nunca más enviará dinero por transferencia sin llamar al destinatario para verificar la información.

"Una conversación telefónica de dos minutos podría haber evitado todo esto", dice Myers.