NO DEJE QUE SU CLIENTE SEA VÍCTIMA DEL FRAUDE DE TRANSFERENCIA ELECTRÓNICA MÁS RECIENTE.

APRENDA A PROTEGERSE Y AYUDE A PROTEGERLOS.

En meses recientes, los profesionales de bienes raíces han reportado el aumento de un fraude de transferencia particularmente insidioso. Un hacker entra en la cuenta de correo electrónico de un titular para obtener información sobre las próximas transacciones de bienes raíces. Después de monitorear la cuenta para determinar el probable momento del cierre, el hacker envía un correo electrónico al comprador, haciéndose pasar por el representante de la compañía de título o el titular. El correo electrónico fraudulento contendrá nuevas instrucciones de transferencia o información de ruta, y solicitará que el comprador envíe los fondos relacionados con la transacción de acuerdo con ellas. Por desgracia, algunos compradores han caído en este ardid, y han perdido dinero.

Una posible señal de alarma a la que tenemos que estar atentos, y sobre la cual alertar a los clientes, es cualquier referencia a una transacción de "transferencia SWIFT", un término que indica un destino internacional para los fondos. Sin embargo y a diferencia de muchos otros esquemas de "phishing" basados en correo electrónico, esta modalidad en particular parece ser más sofisticada y se menos reconocible como fraude. Las comunicaciones no contienen la gramática típica o las rarezas de estilo que están a menudo presentes en los correos electrónicos fraudulentos. Además, debido a que el perpetrador ha estado monitoreando la cuenta de correo electrónico del titular, la comunicación fraudulenta puede incluir información detallada y precisa relacionada con la transacción inmobiliaria, incluyendo datos sobre la transferencia y detalles bancarios, números de expediente, fechas clave, nombres y direcciones. Finalmente, los correos electrónicos pueden provenir de lo que parece ser una dirección de correo electrónico legítima, ya sea porque el ladrón ha creado exitosamente una cuenta falsa que contiene el nombre de un negocio legítimo, o porque está enviando el correo electrónico desde una cuenta genuinamente legítima, aunque haya sido hackeada.

Tenga en cuenta, además, que este esquema en particular es solo una de las muchas formas de fraude en línea que se cometen contra los titulares de bienes raíces y sus clientes. Para proteger a todas los involucrados en una transacción inmobiliaria contra el cibercrimen, he aquí algunos consejos para que usted y sus clientes eviten convertirse en víctimas del fraude electrónico:

1. NUNCA envíe información financiera delicada por correo electrónico sin CIFRARLA. Explicaremos qué es y cómo puede realizarse el CIFRADO en la contraportada de este artículo.
2. Antes de transferir fondos, debe ponerse en contacto con el destinatario previsto a través de un número de teléfono verificado y confirmar que la información de transferencia sea correcta. No confíe en los números de teléfono o direcciones de sitios web proporcionados en un correo electrónico no verificado.
3. Limpie su cuenta de correo electrónico con regularidad. Sus correos electrónicos pueden establecer patrones en su práctica comercial a lo largo del tiempo, que los hackers pueden utilizar contra usted.
4. Cambie sus nombres de usuario y contraseñas con regularidad.
5. Nunca haga clic en enlaces contenidos en un correo electrónico no verificado. Además de dirigirlo a sitios web falsos, estos enlaces pueden contener virus y otro software espía malicioso que puede poner en riesgo su computadora, y sus transacciones, ante posibles ataques.
6. Nunca realice negocios a través de una red Wi-Fi pública no segura, como las disponibles en cafeterías locales y hoteles.
7. Confíe en sus instintos. Diga a los clientes que si un correo electrónico o una llamada telefónica les parecen sospechosos o "extraños", se abstengan de actuar hasta que la comunicación se haya verificado de manera independiente como legítima.
8. Asegúrese de implementar el software antivirus más actualizado en sus computadoras.
9. Proporcione una copia de este artículo a todos los involucrados en las transacciones.
10. Insista en que todas las partes involucradas en la transacción implementen medidas de seguridad.

continuación

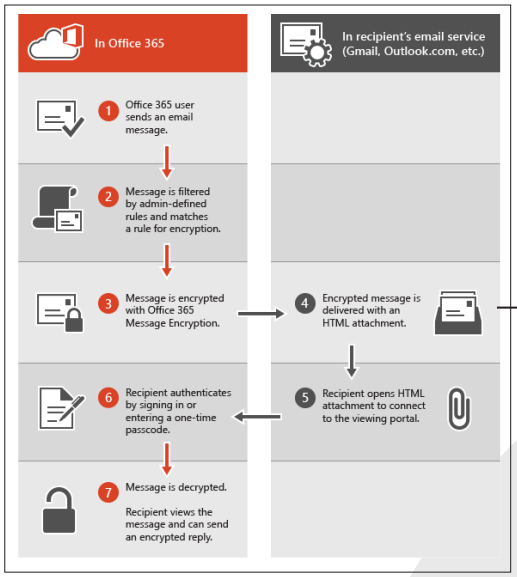
CHICAGO TITLE®

¿QUÉ ES EL CIFRADO DE CORREO ELECTRÓNICO Y CÓMO FUNCIONA?

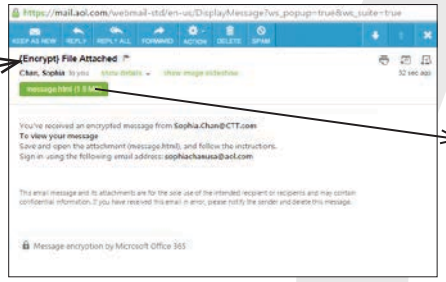
El cifrado es el proceso mediante el cual la información se codifica de manera que solo un destinatario autorizado puede decodificar y consumir la información. Así es cómo funciona comúnmente el cifrado de correo electrónico:

- Un mensaje se cifra, es decir, se transforma de texto simple en un texto cifrado ilegible, ya sea en el equipo del remitente o por un servidor central mientras el mensaje está en tránsito.
- El mensaje permanece en formato cifrado mientras está en tránsito, con el fin de protegerlo de ser leído en caso de que el mensaje sea interceptado.
- Una vez que el destinatario recibe el mensaje, este se transforma de nuevo en texto simple legible de una de dos maneras:
  1. El equipo del destinatario utiliza una clave para descifrar el mensaje, o
  2. Un servidor central descifra el mensaje en nombre del destinatario después de validar su identidad.

A continuación se muestra un diagrama de *Microsoft Office 365* que ilustra el proceso de entrega. Chicago Title utiliza *Office 365* como servidor central.



Un mensaje cifrado por Office 365 Message Encryption se ve así...



Todos los mensajes de correo electrónico cifrados tendrán {Encrypt} en la línea del asunto.

Ahora contiene un archivo adjunto en HTML.

Un mensaje de correo electrónico cifrado llega a la bandeja de entrada del destinatario con un archivo adjunto en HTML. Después de abrir el archivo adjunto, los destinatarios ven instrucciones para abrir y ver el mensaje. Sin importar su tipo de servicio de correo electrónico, la experiencia es la misma. El destinatario puede optar por iniciar sesión con una cuenta de trabajo asociada con Office 365, con una cuenta de Microsoft. Como alternativa, el destinatario puede optar por utilizar un código de un solo uso si, por ejemplo, no tiene una cuenta de trabajo o una cuenta de Microsoft y no desea crear una nueva cuenta de Microsoft.

INSTRUCCIONES PARA CREAR UNA CUENTA U OBTENER UN CÓDIGO DE UN SOLO USO

PARA CREAR UNA CUENTA (Solo unos minutos de su tiempo pueden significar salvar su información o la de su cliente frente a los hackers)

1. Siga las instrucciones contenidas en el mensaje de correo electrónico para guardar el elemento adjunto.
2. Abra el archivo mensaje.html y seleccione "Iniciar sesión". Si aparece un mensaje que le pregunta si desea enviar información a una página externa, seleccione Aceptar. Tal vez necesite también permitir las ventanas emergentes, en caso de que su navegador las bloquee.
3. Inicie sesión en el portal de cifrado con una cuenta de Microsoft, como se indica en el mensaje. Si no tiene una cuenta de Microsoft, puede elegir la opción de crear una asociada con su dirección de correo electrónico. (Deberá llenar un formulario y efectuar un paso de verificación). Para ver el mensaje cifrado, la dirección de correo electrónico de la cuenta de Microsoft debe coincidir con la dirección a la que se envió el mensaje cifrado.

   NOTA: si ya inicio sesión, no tendrá que hacerlo de nuevo.
4. Después de iniciar sesión, podrá ver el contenido del mensaje cifrado.

PARA OBTENER UN CÓDIGO DE ACCESO DE UN SOLO USO

1. Siga las instrucciones contenidas en el mensaje de correo electrónico para guardar el elemento adjunto.
2. Abra el archivo mensaje.html y seleccione "Usar un código de acceso de un solo uso".
3. Se le enviará el código de acceso en un mensaje de correo electrónico. Obtenga el código de acceso, ingréselo en el recuadro proporcionado y luego haga clic en CONTINUAR.
4. Ahora podrá ver su mensaje.

   NOTA: cada código de acceso se vence después de 15 minutos. Si eso ocurre, o si no puede abrir el mensaje por algún motivo, vuelva a comenzar abriendo el archivo adjunto de nuevo y siga los pasos. Asegúrese de que el código de referencia en el correo electrónico que contiene el código de acceso coincida con el código de referencia en el portal.

¿SABÍA QUE...? Al enviarnos información confidencial, siempre puede RESPONDER AL correo electrónico cifrado que le enviamos y la información también se cifrará automáticamente. Si aún no cuenta con uno, simplemente pida a su agente de fideicomiso que inicie un mensaje de correo electrónico cifrado y se lo envíe, guarde el correo electrónico y úselo para todas las futuras comunicaciones relacionadas con esa transacción en particular.

Para conocer medidas adicionales sobre cómo protegerse tanto a usted como a sus clientes, visite www.onguardonline.gov.

Esta información llega a usted gracias a: