

DON'T LET  
YOUR CLIENT BE THE  
**VICTIM**  
OF THE LATEST  
WIRE TRANSFER SCAM.



LEARN HOW TO PROTECT YOURSELF AND **HELP PROTECT THEM.**

In recent months, real estate professionals have reported an upswing in a particularly insidious wire scam. A hacker will break into a licensee's e-mail account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a close, the hacker will send an e-mail to the buyer, posing either as the title company representative or as the licensee. The fraudulent e-mail will contain new wiring instructions or routing information, and will request that the buyer send transaction-related funds accordingly. Unfortunately, some buyers have fallen for this scheme, and have lost money.

A possible red flag to be aware of, and to alert clients to, is any reference to a "SWIFT wire" transaction, a term that indicates an overseas destination for the funds. However, unlike many other e-mail-based "phishing" schemes, this particular manifestation appears to be more sophisticated and less recognizable as fraud. The communications do not contain the typical grammatical or stylistic oddities that are often present in scam e-mails. In addition, because the perpetrator has been monitoring the licensee's e-mail account, the fraudulent communication may include detailed and accurate information pertaining to the real estate transaction, including existing wire and banking information, file numbers, and key dates, names, and addresses. Finally, the e-mails may come from what appears to be a legitimate e-mail address, either because the thief has successfully created a sham account containing a legitimate business's name, or because he or she is sending the e-mail from a truly legitimate—albeit hacked—account.

Be aware, also, that this particular scheme is only one of many forms of online fraud being perpetrated against real estate licensees and their clients. In protecting all parties to a real estate transaction from cybercrime, here are some advises for you and your clients to protect yourselves from becoming a victim to wire fraud:

1. NEVER send any sensitive financial information via e-mail without ENCRYPTING it. We will explain what and how ENCRYPTING can be done on the back page of this article.
2. Prior to wiring any funds, you should contact the intended recipient via a verified telephone number and confirm that the wiring information is accurate. Do not rely on telephone numbers or Web site addresses provided within an unverified e-mail.
3. Clean out your e-mail account on a regular basis. Your e-mails may establish patterns in your business practice over time that hackers can use against you.
4. Change your user names and passwords on a regular basis.
5. Never click on any links in an unverified email. In addition to leading you to fake websites, these links can contain viruses and other malicious spyware that can make your computer – and your transactions – vulnerable to attack.
6. Never conduct business over unsecured public wifi such as those available at your local coffee shops and hotels.
7. Trust your instincts. Tell clients that if an e-mail or a telephone call ever seems suspicious or "off," that they should refrain from taking any action until the communication has been independently verified as legitimate.
8. Make sure to implement the most up-to-date anti-virus software installed on your computers.
9. Provide a copy of this article to everyone on the transactions.
10. Insist all parties on the transaction to have security measure in place.

*cont'd*



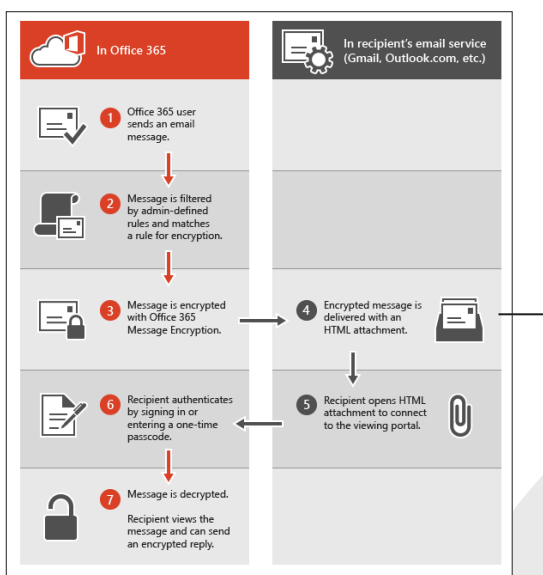
**CHICAGO TITLE**

## WHAT IS EMAIL ENCRYPTION AND HOW DOES IT WORK?

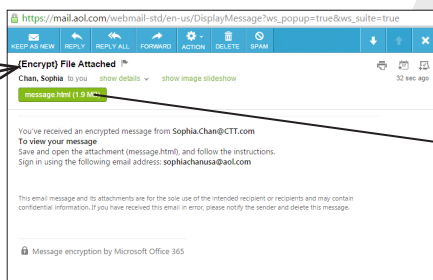
Encryption is the process by which information is encoded so that only an authorized recipient can decode and consume the information. Here's how email encryption typically works:

- A message is encrypted, or transformed from plain text into unreadable ciphertext, either on the sender's machine, or by a central server while the message is in transit.
- The message remains in ciphertext while it's in transit in order to protect it from being read in case the message is intercepted.
- Once the message is received by the recipient, the message is transformed back into readable plain text in one of two ways:
  1. The recipient's machine uses a key to decrypt the message, or
  2. A central server decrypts the message on behalf of the recipient after validating the recipient's identity.

Below is a diagram from *Microsoft Office 365* that illustrates the delivery process. Chicago Title utilizes *Office 365* as our central server.



A message that is encrypted by Office 365 Message Encryption looks like this...



All Encrypted email messages will have this **(Encrypt)** on the subject line.

It now contains an HTML file attachment.

## INSTRUCTIONS TO CREATE AN ACCOUNT OR OBTAIN A ONE-TIME CODE

**TO CREATE AN ACCOUNT** (Only a few minutes of your time can mean saving you or your client's information from the hackers)

1. Follow the instructions in the email message to save the attachment.
2. Open the message.html file and select "Sign in". If a message appears that asks if you want to submit information to an external page, choose OK. You may also need to allow pop-ups, if your web browser blocks them.
3. Sign in to the encryption portal with a Microsoft account, as instructed in the message. If you don't have a Microsoft account, you can choose the option to create one associated with your email address. (You'll have to fill out a form and complete a verification step.) In order to view the encrypted message, the email address for the Microsoft account must match the address to which the encrypted message was sent.

**NOTE: If you're already signed in, you won't have to sign in again.**

4. After signing in, you can view the contents of the encrypted message.

### TO OBTAIN A ONE-TIME PASSCODE

1. Follow the instructions in the email message to save the attachment.
2. Open the message.html file and select "Use a one-time passcode".
3. The passcode is sent to you in an email message. Get the passcode, enter it into the box provided, and then click CONTINUE.
4. You can now view your message.

**NOTE:** Each passcode expires after 15 minutes. If that happens, or if you can't open the message for any reason, start over by opening the attachment again and following the steps. Make sure the reference code in the email containing the passcode matches the reference code in the portal.

**DO YOU KNOW?** When sending sensitive information to us, you can always **REPLY TO** the encrypted email we sent you and the information will also be encrypted automatically? If you don't already have one, simply ask your escrow officer to initiate an encrypted email message and send to you, save the email and use it for all future communication for that particular transaction.

For additional steps on how you can protect yourself and your clients, click here to download "[Steps you can take to avoid being a target of wire fraud scams.](#)" We also recommend visiting this website for useful information: [www.onguardonline.gov](http://www.onguardonline.gov) and if you are looking for solutions to send encrypted emails [click here for more information.](#)

This information is proudly brought to you by:

An encrypted email message arrives in the recipient's inbox with an HTML attachment. After opening the attachment, recipients see instructions for opening and viewing the message. Regardless of their type of email service, the experience is the same. The recipient can choose to sign in with a work account associated with Office 365, with a Microsoft account. Alternatively, the recipient can choose to use a one-time passcode if, for example, they don't have a work account or a Microsoft account and don't want to create a new Microsoft account.