Wire Fraud Is Here to Stay and Play

In the last few years, we have been bombarded with news stories on how companies worldwide fall victim to wire fraud. Wire fraud's presence in the real estate market is a little too close for comfort. In 2017 alone, the FBI reportedly received 301,580 complaints [and] losses exceeded $1.4 billion […] in the real estate/rental sector* for wire fraud. These figures are not necessarily surprising, as the housing market is worth an estimated $33.3 trillion.** This astronomical number is quite tempting to the bad guys, because it potentially means a great payday for them. To prevent them from siphoning any types of funds, we need to start with the basics and understand the game that the bad guys seek to play.

First, ***it all starts with a simple phishing e-mail***. This email can be sent to essentially anyone. Below you will find a breakdown of events that ***can*** occur with a wire fraud transaction:

1. The bad guy sends an e-mail to an unsuspecting user. Let's say this user is a real estate attorney and the criminal came across the attorney's information online.
2. The bad guy asks this user to click on the "harmless" link below, because the sender suspects that something is wrong with the user's email account.
3. Following these orders, the attorney clicks on the link and is prompted to select the email provider that the attorney has (Outlook, Yahoo!, Gmail, etc.).
4. Once he clicks on the provider he has, he gets presented with a login screen that looks strikingly similar to his current provider's page.
5. He proceeds to type in his credentials, and he quickly receives a message that says, "incorrect username and password."
    - This message is vital in the scheme, because the user will likely think to himself, "Okay, I thought I entered my credentials properly, but they are apparently incorrect." While the attorney dwells on this thought, the bad guy has already captured this user's username and password in the background on a separate portal.
6. The bad guys advance in their adventure and maliciously log in to this attorney's actual email account without the attorney ever knowing.
7. Since bad guys tend to play a waiting game, they hide and see what types of emails this attorney is receiving.
8. They notice that this attorney is discussing an impending closing with a client and has asked the client to wire $10,000 to an ABC Bank in Connecticut. This attorney also provides the client with a correct routing and account number.
9. The following day, the client receives another e-mail from the "attorney," which notes a slight change in wiring these funds. This "attorney" tells the client to wire the $10,000 to an ABC Bank in Texas. Upon this request from the "attorney," the client wires out the money; and thus, a wire fraud transaction is born.

As always, it is important to remain alert and to be suspicious of the red flags below in your attempts to minimize the risk of wire fraud:

- Check for grammatical mistakes within the email.
    - Yes, it is true that the bad guys hire others to check their grammar, but, remember, even the best cybercriminals mess up!
- Be on the lookout for odd introductions:
    - "Dear Sir/Madam" or "Hi, kindly review."
- Ask yourself, "Was I expecting something from this sender?"
- Examine urgent requests and **ANY** changes to wiring instructions. If there are changes present, remember to **CALL** and **VERIFY** using a known number found online and *not* within the sender's e-mail signature.
- Check timestamps of emails and question the fact that it is strange for the client to be emailing you at 2:00 A.M.
- Check the domains of senders.
    - If the email is coming from your clients and their known email address is "jsmith@gmail.com," make sure that your correspondences with them say the above email and not "jsmith@gmmail.com."
- Hover over all links to ensure that they are going to the intended website.
- Trust your GUT!

***Caution:** This outline of a potential wire fraud scenario is only one of the many ways that the bad guys can compromise one's account. Since the cybercriminal network changes, essentially every day, it is difficult to consistently keep up with the multiple tactics they use to try to siphon funds, and possibly data, from innocent people.*

Please contact security@catic.com if you have any questions.

*Forbes.com

**Housingwire.com