The Myths, Dangers, and Risks of Encrypted Email in Real Estate

The real estate industry is constantly bombarded by cyber attacks, many of which target the transfer of closing costs from the home buyer to the title company. The frequency of these attacks rose 480% in 2016 alone, and attacks mostly involve email and/or phone spoofing. Title companies are increasingly turning to encrypted/secured email to protect their buyers from wire fraud. Unfortunately, encrypted/secured emails can do nothing to prevent the biggest threats that are defrauding home buyers. It is a dangerous myth that encrypted/secured email protects home buyers and lenders from wire fraud.

So, what is encrypted/secured email, how is it used in real estate, and why does it not prevent wire fraud?

History

Email encryption is nearly as old as email itself. PGP, a common protocol for email encryption, was initially released in 1991. Since email encryption is so old, why aren't all emails encrypted? The simple answer is that it costs money, increases complexity, and isn't needed for all email.

How it works

Encrypted email was developed to prevent man-in-the-middle snooping of emails. Typically, encrypted email is deployed within companies/organizations to prevent outsiders from reading their emails in the event that a hacker gains access to their network. In this scenario, both the sender and receiver use the same encryption protocol.

But what happens when a receiver is with a different organization, or uses a personal account, as is often the case for real estate transactions? Well, standard email encryption in the real estate industry uses what is known as "opportunistic encryption." This means the email servers attempt to send encrypted emails, but simply fall back to unencrypted emails if the receiver does not support the same encryption protocol as the sender. In this case, emails aren't encrypted at all.

In this case, emails aren't encrypted at all.

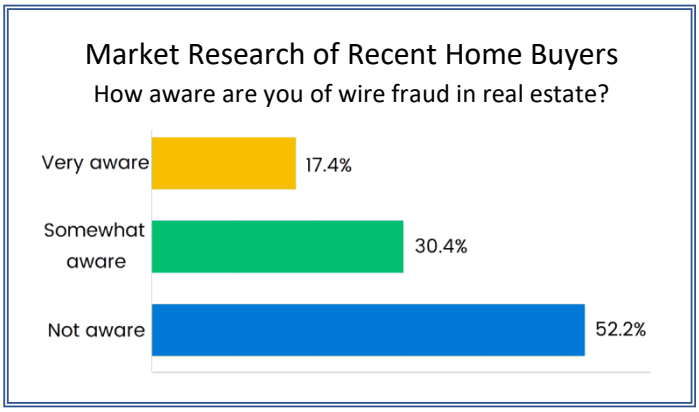
Another possibility is that the email remains encrypted, and a link is sent to the receiver which directs them to a web-based service to retrieve their email. Not only does the receiver have to visit a website, they must also register an account, thus requiring another username and password. All of this is cumbersome for no apparent benefit to the receiver.

How is encrypted email perceived to prevent wire fraud?

Title companies are increasingly turning to encrypted email to share wire transfer instructions with their clients (home buyers and lenders). The process typically consists of a series of phone calls and encrypted emails between the title company and the home buyer. A process for a conscientious title company may look like the following:

- Title company attempts to educate the home buyer on the dangers of wire fraud.
- Title company instructs the home buyer to call for wiring instructions, be suspicious of emails with wiring instructions, and call the title company to verify. All phone calls should be to a 'known' number not listed in the email.
- Once the home buyer calls the title company, the title company sends an encrypted email to the home buyer with the wiring instructions. The home buyer then verifies the wiring instructions, via phone, with the title company.

The previous procedure assumes the home buyer is well aware of the dangers of wire fraud in real estate. Market research shows that **only 17% of recent home buyers are 'very aware' of the dangers of wire fraud** in real estate. This is especially alarming since these are recent home buyers, who have been made aware of the dangers (or should have been) when they purchased their home.



In the previous procedure, the only thing encrypted email has done is prevent a hacker from seeing the contents of the wire transfer instructions (which are not sensitive to begin with). The encrypted email has done nothing to protect the home buyer from fraud.

Lastly, the previous procedure educates the home buyer to expect wiring instructions via email. This actually makes home buyers more susceptible to spoofed or cloned emails since they are actively expecting an email with wiring instructions.

Why doesn't encrypted email prevent wire fraud?

Encrypted email protects the contents of an email, but that does not protect against wire fraud in real estate. The biggest threats to secure wire transfers are compromised accounts, email spoofing, and clone phishing. Unfortunately, none of these threats are addressed by encrypted email.

The biggest threats to secure wire transfers are compromised accounts, email spoofing, and clone phishing. Unfortunately, none of these threats are addressed by encrypted email.

Compromised accounts

A compromised account is an account that has been accessed by someone other than the owner (i.e. a hacker has your login and password). Email accounts can be compromised through many methods such as brute-force attacks, hacked websites, weak passwords, similar passwords for multiple services, password sharing, and social engineering.

Compromised email accounts may include accounts from title companies, realtors, lenders, or home buyers. There are many email accounts, and thus many targets, involved in closing a real estate transaction. Hackers use compromised accounts to intercept wire information, and/or send and resend wire information.

With a compromised title company account, a hacker can send an encrypted email with wire instructions that is from the title company itself. Or, the hacker can attack the home buyer's email accounts and intercept/delete any wire information emailed from the title company (including encrypted email) and insert their own wire information. Even worse, the hacker will call the home buyer pretending to be the title company and then send the fraudulent wire information. Or, the hacker will send an email to the home buyer saying "don't forget to call for your wire information," while subtly leaving a fraudulent phone number in their email signature.

There are many targets for compromised email accounts, including title company employees, realtors, lenders, and home buyers. When the buyer is expecting wire information via email, they are unsuspecting when they receive wire information via email from one of these compromised accounts. **Unfortunately, encrypted email cannot protect against any of these accounts being compromised.**

Email spoofing

Email spoofing is the creation of emails with a forged email header (i.e. sender address). Email spoofing is possible because the core email protocols (SMTP – Simple Mail Transfer Protocol) do not have mechanisms for authentication. This is one reason the FTC and FBI urge everyone to avoid email when sharing private or financial information.

This is one reason the FTC and FBI urge everyone to avoid email when sharing private or financial information.

In real estate, hackers send spoofed emails to home buyers that appear to be from the title company, realtor, or lender. Spoofed emails are continually becoming more elaborate and harder to detect. Gone are the days of many misspelled words and poor grammar. With so much money on the line, hackers are creating very sophisticated and targeted spoofed emails. Often, the spoofed emails will have a legitimate name and email in the 'From' and 'Reply-to' fields.

Clone phishing

Another form of spoofing doesn't even involve forging the name or email address. In this scenario, the hacker creates an email account that looks extremely similar to the account they are impersonating. For example, instead of receiving an email from "Andy White <andy@wellstitle.com>", the hacker will create an email account for "Andy White <andy@vvellstitle.com>". In this case, the 'w' in 'wellstitle' has been replaced with two 'v's which can be difficult to notice even for experienced security experts.

Cloned emails are so sophisticated and targeted, often the email signatures of the title companies are copied directly to the cloned email. Even pictures of the escrow agent/officer are inserted. One recent case involved the title company phone number only being changed by a single digit.

With home buyers expecting the wire information to be emailed, they are unsuspecting when an email arrives with wire information appearing to be from the title company. A spoofed or cloned email can also appear to be encrypted (or can actually be encrypted). Therefore, email encryption can do nothing to protect against spoofed or cloned emails.

Therefore, email encryption can do nothing to protect against spoofed or cloned emails.

In summary, for end-to-end email encryption to be enforced, the home buyer must support the same encryption protocol as the title company. Since this is rarely the case, to maintain end-to-end encryption, users must register an account to access the encrypted email. Most users do not enjoy the hassle of one more registration/password. The other alternative is that end-to-end encryption is not maintained. This is easier for the home buyer but eliminates the point of encrypted email. Regardless, no type of encrypted email protects home buyers from the major threats of wire fraud: compromised accounts, email spoofing, and clone phishing.

Conclusion

Does your current wire information procedure protect against compromised accounts and email spoofing? If you're only using encrypted email and phone calls, the answer is no. When emails are used to transmit wire transfer information, three major threats exist: compromised accounts, email spoofing, and clone phishing. Encrypted email does not and cannot protect against any of these threats. BuyerDocs provides a web-based solution which eliminates email (encrypted or normal) for sharing wire transfer information, thus protecting home buyers from wire fraud.

About the Author

Andy White, Ph.D. is the Co-founder and CEO of BuyerDocs. He holds a Master of Electrical Engineering degree, along with a Ph.D. in Computer Engineering. He has multiple publications in the computer technology field, and is the inventor on 12 patent applications in the computer hardware and software industry. Contact Andy at andy@buyerdocs.com

BuyerDocs provides a web-based service for protecting home buyers from wire fraud in real estate.