September 2016

THE GIARDINELLI LAW GROUP, A P C

Courtside Newsletter

Cybersecurity: How Can You Protect Yourself as a Real Estate Broker or Agent?

BY: JOHN V. GIARDINELLI, ATTORNEY AT LAW
ASHLEY PLANCHON, LAW CLERK
CASEY MCINTOSH, PARALEGAL

Before recent years, cybersecurity sounded like something out of a science fiction movie—as though you need to protect yourself from robots gone rogue. While we are not necessarily running from awry artificial intelligence ("AI"), threats to cybersecurity are real and the need to protect yourself both personally and professionally is great.

What is "cybersecurity"?
According to the University of Maryland University College, "Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction." Businesses store and transmit a great deal of confidential and Personally Identifiable Information ("PII") on their computers and online, making them vulnerable to cybersecurity attacks by hackers and fraudsters. Sensitive PII, which could result in harm to the individual if disclosed to the wrong people, includes Social Security numbers ("SSNs"), passport numbers, drivers' license numbers, financial information, unique identifiers, medical information, and biometric information.

How is the real estate industry involved?
According to the National Association of REALTORS® ("NAR"), although most headlines we see about cybersecurity breaches involve major retailers and/or government figures, the reality is that small- to mid-size businesses make up the majority of cyberattack victims. Unfortunately, this has also begun to ring true for real estate brokerages and their clients. In a field where more activities are being conducted online, including the transfer of clients' funds, fraudsters are more apt to target brokerages to conduct their schemes.

Recently, there has been a spate of attacks on wire transfers by well-informed fraudsters. The fraudster will hack into a licensee's email account to obtain information on upcoming real estate transactions. Then, like the proverbial wolf in sheep's clothing, the fraudsters will pose as the title company representative or the licensee and send an email to the buyer providing new wiring instructions or routing numbers for the buyer to utilize. This sort of fraud has been much more difficult to recognize than traditional phishing schemes due to the fact that the email to the buyer will either come from a sham account that looks legitimate, or from a hacked email account. Fraudsters have also been able to set up phone numbers and call centers for buyers to call to verify the wiring instructions. Sellers have had their sale proceeds taken in a similar manner. The money will only stay in the fraudulent account for a moment before being transferred elsewhere, and finding the perpetrators has proven to be difficult.

How can real estate brokerages and agents protect themselves?
Buying, selling or renting a home is an activity that is already fraught with stress. Many people think they are safe working with their brokerages, and transferring funds to and from accounts is the last thing they need to worry about. As their agent or broker, it is up to the real estate professional to protect his clients. This is not only an ethical obligation, but also a smart move to protect one's business from liability if something malicious does occur. While the brokerage may not be found liable in a lawsuit, it is still costly to defend oneself once a lawsuit has been filed.

California Association of REALTORS® ("C.A.R.") Wire Fraud Advisory
The Wire Fraud Advisory ("WFA") is a new form introduced by the C.A.R. in June of this year. According to C.A.R., the buyer should receive this form "no later than when the offer to purchase is made" (emphasis added). Since the seller does not generally need to wire funds immediately, the listing agent can provide the form when the seller fills out his disclosures.

The single-page form advises buyers and sellers (in bold type):

1. Obtain the phone number of the Escrow Office at the beginning of the transaction.
2. DO NOT EVER WIRE FUNDS PRIOR TO CALLING YOUR ESCROW OFFICER TO CONFIRM WIRE INSTRUCTIONS. ONLY USE A PHONE NUMBER YOU WERE PROVIDED PREVIOUSLY. Do not use any different phone number included in the emailed wire transfer instructions.
3. Orally confirm the wire transfer instruction is legitimate and confirm the bank routing number, account numbers and other codes before taking steps to transfer the funds.
4. Avoid sending personal information in emails or texts. Provide such information in person or over the telephone directly to the Escrow Officer.
5. Take steps to secure the system you are using with your email account. These steps include creating strong passwords, using secure WIFI, and not using free services.

Continued …

Passwords

While we have all heard the tips and tricks for creating a strong password and keeping it safe, they bear repeating since fraudsters have been known to hack agents' email accounts:

- Passwords should be at least eight characters—the longer the password, the harder it is for hackers to crack.
- Include numbers, capital letters, and symbols. Use a "@" for an "a," or a "$" for an "s." Commas, apostrophes, and hyphens can even be used. Randomly capitalize letters throughout the password, not just in the beginning of a word.
- Use shortened phrases, sentences or codes, such as "Be$t_of-TimEs" ["Best of times" (from the first sentence in *A Tale of Two Cites*)].
- Make shapes with the keyboard. "6TfvBhy^" makes a diamond shape.
- "I love soccer, running, football and food" could be shortened to "Il$crRng*tBl&Fd."
- Don't use words that can be found in a dictionary. Hackers have software to automatically plug common words into password fields (this technique is called a "dictionary attack"). The same goes for words spelled backwards, common misspellings, and slang terms.
- Don't use your spouse's name, kids' names, dog's name, your name, your date of birth, parents' names, favorite color, or favorite song. In short, don't make it obvious.
- Don't use the same password for everything. Change it up from site to site. According to McAfee, "two recent breaches [of cybersecurity] revealed a password reuse rate of 31% among victims."
- Don't share your passwords with anyone, especially not over the phone.
- Don't leave your password in plain sight or in an obvious location, such as on your computer monitor, under your mousepad, or in a desk drawer.
- Change your password regularly.
- Check the strength of your password in an online password strength tester.
- Create a tip sheet to help remember your passwords, rather than a cheat sheet containing the password itself. The tip sheet will tip you off to what your password is, but will still be safe if it falls into the wrong hands or gets lost.

Passphrases

In spite of all these tips, passphrases have been proven to be superior to passwords as they are stronger, easier to remember and more difficult for hackers to guess. Passphrases are 20-30 characters in length (versus the 8-12 of a password), and contain entropy (aka randomness). This entropy is key to creating a strong passphrase that hackers cannot plug into software to discern. Ultimately, a passphrase is exactly what is sounds like—a set of randomly selected phrases used as a password.

Diceware for passphrases:

To ensure randomness, Diceware has created a wordlist of 7,776 English words that correspond to a five-digit number (http://world.std.com/~reinhold/dicewarewordlist.pdf). Like the name suggests, you will need dice for this. (Not to worry if you don't have a physical die. Type "roll a die" in Google, and a die roller will appear.)

- Roll the dice five times, writing down the number you get each time.
- Look up the corresponding word on the Diceware word list. (For example, "26235" corresponds with "forte.")
- Repeat this at least 3 times for your passphrase. (Example: "forte stu dk")
- For a stronger passphrase use more words.

These phrases are much easier to memorize than a password with random characters, letters and numbers because the human brain can associate them with something. The passphrase "forte stu dk," reminds me of a piano (forte), Stu for a person's name, and a duck (without the middle letters). Random word association, to be sure, but whatever works.

Data Security Program

Having a comprehensive data security program is vital for a real estate brokerage. The Federal Trade Commission has issued a brochure entitled "Protecting Personal Information: A Guide for Business," which can be found online at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security. The 5 key principals are:

1. Take stock. Know what information you have in your files and on your computer.
2. Scale down. Only gather the PII that your brokerage needs.
3. Lock it. Keep PII limited to only the individuals who need it. Any hard copy forms and information should be kept in a locked file cabinet and only authorized individuals should have access to the key. Digital information should be kept on a locked computer or on an encrypted drive.
4. Pitch it. California law requires a real estate broker to retain all documents obtained in connection with a real estate transaction for 3 years. This retention period runs from the date of closing, or the date of the listing if the transaction is not consummated. (Business & Professions Code § 10148). After the expiration of this retention period, a broker should shred paper documents, erase electronic records and drives, or otherwise modify the personal information on any records to make it unreadable or undecipherable through any means. (Civil Code § 1798.81).
5. Plan ahead. Know what you'll do if a security breach does occur: how will you inform clients? Who will you reach out to in order to rectify the breach and prevent it from happening again?

C.A.R. and NAR also offer resources that expound on the sort of data security program that REALTORS® should implement:

- "Data Security and Privacy Toolkit" National Association of REALTORS®, available at http://www.realtor.org/topics/data-privacy-and-security/resources
- "Protect Your Brokerage from Cybercrime" Member Legal Services (June 29, 2016), available at http://www.car.org/legal/broker-practice-folder/cybercrime/

* * *

This article was just the tip of the iceberg when it comes to the amount of information and advice available for real estate brokers and agents to protect themselves from cybercrime. If you or your clients feel you are a victim of cybercrime, contact your local law enforcement agency and REALTOR® association, as well as report the issue to the Department of Justice. In a field built on trust, it is always better to be safe than sorry. Hopefully some of the above tips will assist in protecting you and your clients from some of the seedier characters in the world.