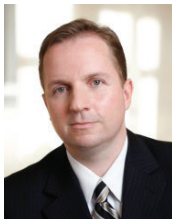
Not Just Politics: Email Hacks Also Impacting the NYC Real Estate Market

By Michael J. Romer, Esq., Romer Debbas LLP



We now live and work in a world where emails are hacked and information is stolen on a regular basis. It seems there is a new story concerning email hacks every day. As we have all come to learn, top-secret government emails aren't even truly safe in today's day and age. Sadly, one's personal and financial information has become a commodity of sorts. However, many don't realize that the real estate market is not immune to hacking, fraud and information theft.

Over the course of my 16 years of practice, I have been witness to multiple attempted scams ranging from fake official bank checks (that look almost exactly like the real thing) to attempted fraudulent property transfers. This is why it's so crucial to ensure that banks, title companies and other business partners are both trusted and experienced. Such attempts at fraud and theft are generally easy to detect and prevent. However, email hacking has taken things to a different level. In many cases, despite the best servers and IT available, we practitioners often cannot trust the information we are receiving on a daily basis from our own colleagues in the field.

In recent months, we have received multiple emails from practicing lawyers' actual email accounts, which were later proven to be fraudulent. Besides potentially wanting to obtain personal information from a client for identity theft purposes (which alone is concerning), it seems the individuals behind the hacks are zeroing in on wiring instructions.

Here is the scam in a nutshell: An individual hacks the email server of a real estate lawyer (often a personal one) and scans the emails searching for a deal at the wiring money stage (i.e. time of down payment posting or time of closing). Then the hacker composes an email from the attorney's server and email address providing the wiring instructions for the account to which either the contract down payment, closing proceeds or otherwise should be sent. The problem is that the account number pertains to a bank account (usually offshore) maintained by a shell company affiliated with the hacker. If the email recipient (generally the attorney on the other side) or its bank does not verbally verify the wiring instructions and then proceeds to send the wire, those funds could very well disappear. Substantial sums of money are at risk on a daily basis and all parties to a deal are forced to be more diligent than ever before.

For years, I have quietly questioned why practicing real estate attorneys in New York City would operate with personal email servers such as Gmail, AOL or Yahoo, to name a few. I have also wondered why real estate brokers and their clients would feel comfortable hiring an attorney with such an email. Although I am respectful of the business practices of others and believe to each his own, I have always felt this was a risky practice, jeopardizing privileged and confidential information concerning multi-million dollar transactions. Exchanging information via email with another attorney who uses a personal email server always felt a bit odd to me. Last month, we encountered a situation proving it not just odd but extremely dangerous.

Our office was representing a purchaser acquiring a piece of property and was working with an attorney on the other side (whom we have worked with before) and the contract had just been finalized and executed by our client. Our client (as many do) wired the down payment proceeds to us as counsel in order for us to forward over to seller's counsel. This particular attorney requested the down payment be wired to his escrow account. Shortly thereafter, we received a second email from the exact same email address stating that the previous instructions were sent in error and that we were to use replacement instructions. As we always do (and I cannot stress the importance of this), our office contacted the other attorney to verbally verify the instructions and we were surprised to learn that the second email was indeed fraudulent. Someone had hacked the attorney's email server (which happened to be personal), read the email chain, and sent instructions that matched the initial one's except both the bank account number and the routing number had been changed. Luckily, a crisis was averted.

With respect to our market, it begs the question as to what measures real estate attorneys, law firms, brokerage houses, banks and otherwise should have in place to prevent emails from being hacked. A wide majority of banking institutions has even implemented password-protected secure email systems requiring an email recipient to create his own login and password to access the bank's secure server. Although we have always maintained a secure and monitored email server, as a firm representing many institutional lenders, we recently implemented a similar "more secure" system to be used when sending wiring instructions. It is an added step and some may find it to be a nuisance; however, we have come to realize that it is a necessary defense to what has become the reality of today's world.

A law firm's biggest responsibility and liability is protecting client funds held in escrow. Despite the best email servers available, it is more crucial than ever to ensure that wiring instructions are always verified and that our banking partners have experienced security teams in place as a second line of defense.

Michael J. Romer, Esq.
Romer Debbas LLP
275 Madison Avenue, Suite 801, New York, NY 10016
212-888-3100 | MRomer@romerdebbas.com
www.romerdebbas.com