WCRE
WOLF COMMERCIAL REAL ESTATE

#InformationFriday

PURCHASING COMMERCIAL REAL ESTATE - HOW TO PROTECT YOUR FINANCIAL DATA

By David J. Humphreys, MS, Security+, CISSP CTO & Principal Security Consultant, Avasek
Kevin Comber, ITIL, CBCP, VP of Business Resiliency, Avasek

May 20, 2016

Regardless if you are purchasing, selling, renting, leasing, or building a commercial property, a wealth of information about you is shared with multiple vendors throughout the transaction. Realtors, Titling Agencies, Real Estate Attorneys, CPAs, and Banks all provide important services when dealing with a real-estate transaction. No one is going to take the security of your data as serious as you, unless it is demanded by compliance requirements OR YOU.

It is time that we, as consumers, start to demand at least the most basic of security controls from the vendors that we work with. After all, the effects of carelessness end up effecting us the most. The rest of this article will dive into a few of these recent cyber scams related to real estate and what we can do to protect ourselves.

SITUATION #1

One of the latest scams in recent months starts when the scammer hacks into a busy real estate agent's email account. The scammer starts watching emails go back and forth waiting for a big sale that is about to close. As closing day nears, the scammer registers a new email address similar to the agents. (i.e. "Josephine Smith" <jsmith@prudental.com> instead of "Josephine Smith" <jsmith@prudential.com> or jkweilin@yahoo.com instead of jkwellin@yahoo.com.) They then email escrow from this email address acting as the listing agent and tell escrow where to wire the funds for the sale. Usually the deed transferring the title has already been completed and escrow closed before the sellers start wondering where their wire transfer is a few days later.

SITUATION #2

People are constantly attached to their cell phones now-a-days. With limited data plans many people will connect to the free Wi-Fi networks at your favorite Starbucks or Dunkin Doughnuts. If you've every connected to one of these before you may realize the next time that you go back it automatically connects. That is because the network has been saved in your device and your device is constantly looking for these networks so that when it finds one it automatically connects. The problem is that a scammer with a $15 transmitting device can "read" the known networks on your devices and the recreate a fake network with the same name, then just like that your device connects and the scammer has access.

SITUATION #3

There have been alerts about particular strands of malware that targets settlement software. The malware is called ZeuS Bot and Zero Access Rootkit, which attacks settlement software and issues checks and moves funds into fictitious files. There have been cases of potential loss exceeding $300,000 per incident.

SITUATION #4

The Consumer Financial Protection Bureau (CFPB) made an advancement in protecting consumer's information last October. CFPB Compliance is one of the largest safeguards protecting consumer data privacy and it requires title agents and other professionals who handle housing transactions to maintain compliance or else face steep financial penalties. The two most important aspects of maintaining compliance is the security and privacy of NP (non-public information) and TILA-RESPA (Truth in Lending Act and Real Estate Settlement Procedures Act). As of October 2015, all financial data transferred via email must be encrypted. (i.e. HUD documents) Unfortunately, 7 months later I have still seen a lack of compliance to this requirement.

follow us:

"Building Successful Relationships" is our Mission.

WCRE
WOLF COMMERCIAL REAL ESTATE

#InformationFriday

HOW TO PROTECT YOURSELF

Doing your due diligence ahead of time when picking entities to help you with your real-estate transaction will not only keep your private information safe. It will ensure that you are working with the leaders in the industry. Those that care about your personal information and understand not only the legal requirements but also the ethical requirements. Which, by-the-way, tend to be the vendors that have mature processes and practices in place to ensure maximum uptime of their services making sure that your transaction goes as smooth as possible. So, here are some tips of what to look for.

These apply to everyone involved. Banks, Real-estate Agents, Title Agencies, CPAs, and Attorneys. You're only as secure as the weakest link.

1) Do not do business with a real-estate agent that uses their personal email addresses from places like yahoo, Gmail, or Aol. This is the sign of "smoke" before a "fire". Using personal email addresses show a lack of appropriate security controls and structure within the organization. They are often more easily hacked due to the lack of organizational control without the mechanisms to monitor for unauthorized access. Sending personal information about yourself to a free email account can expose you to a slew of security concerns.

2) Do they have a security awareness training? This is vitally important these days since most "breaches" are not technical in nature. They are done by the manipulation of the ignorance of a human.

3) Is there written policies and procedures in place to safeguard their client's personal information. Having written policies shows that the company has done their due diligence by at least discussing the risk of taking your personal information on a laptop to the Starbucks for free Wi-Fi. What happens if the laptop is in a vehicle and is stolen? Does their written policy say to take laptops home they must have hard drive encryption? I know it sounds to technical to understand or implement, but here's a little secret. "IT'S NOT ANYMORE" It just takes the adoption of the powers to be. (Sometimes the most difficult of obstacles)

4) Is there a shred policy? At one point your documents are going to be printed. Where do they go after you're done?

5) Do they store client files in a locking file cabinet? Janitorial staff often comes by on nights and weekends when no one is there. A simple cell phone camera clicks and no one knows the difference. Not even a finger print left behind.

6) Do they use public or shared Wi-Fi? Ask then in casual conversation about password policies. You can make a simple remark like "It's such a pain, my company makes me change my passwords every six months. Does yours?" BTW, six months is WAY too long to change passwords ESPECIALLY when dealing with financial data.

7) Don't ever let them fool you by saying "We don't store that information hear onsite. It's all stored there so you have nothing to worry." If they have access to it, that means that anyone that has access to them has access to it!!

8) Ask the agency if what their state's "security breach notification law" is. Every state has one and they SHOULD know what it is.

9) If you see any agent accessing your personal information on a thumb drive, at MINIMUM, ask for a copy of their organizational wide policy. If they don't have one you may want them to review the American Land Title Association (ALTA) guidelines surrounding non-public information (NPI) stating that "The use of removable data devices, like thumb drives, should be either prohibited outright or

follow us:

"Building Successful Relationships" is our Mission.

Wolf Commercial Real Estate
www.wolfcre.com

NJ OFFICE
951 Route 73 North | Suite D
Marlton, NJ 08053
P 856 857-6300 | F 856 283-3950

PA OFFICE
630 Freedom Business Center | 3rd Floor
King of Prussia, PA 19406
P 215 799 6900 | F 610 768 7701

strictly controlled via an organization-wide policy."

10) Ask them to send you a "test" encrypted email. If they cannot do so easily, then that means any backend operations involving YOUR personal information isn't encrypted in compliance with government regulations.

For more information contact:

David J. Humphreys, MS, Security+, CISSP
CTO & Principal Security Consultant
phone: 856.316.4144 x103
Email: david@avasek.com

Kevin Comber, ITIL, CBCP
VP of Business Resiliency
phone: 856.316.4144 x102
email: kevin@avasek.com

AVASEK
Protecting your critical data

follow us:

"Building Successful Relationships" is our Mission.