CYREN

10 Steps to Protect Your Real Estate Business

Solution Brief

Real estate companies of all sizes have become targets for phishing, malware, and ransomware attacks.

According to an FBI report, the hacking of real estate transactions by infiltrating email communications was the fastest growing cybercrime tracked by the agency in 2017, with reported attacks increasing over 50x in value to nearly $1 billion during the year. In a world increasingly dependent on digital technology and with significant amounts of money being transacted, the real estate industry is being challenged by extreme growth in the volume and sophistication of such cyberattacks. Failure to upgrade security adequately can mean severe financial impacts for the victims, and loss of trust and business for the targeted realty firm. These risks are real for both large and small real estate companies, as firms of all sizes face specific and shared industry dynamics.

Industry Dynamics Attract Cyberthreats

High-volume, high-value financial transactions – Wire transfers associated with the closing costs of real estate transactions frequently range into tens of thousands of dollars – and often significantly more – making all participants in the property transaction ripe targets for escrow fraud via sophisticated phishing attacks. With over 80,000 real estate brokerages and over two million active real estate licensees operating in a nearly $500 billion annual property market in the U.S., the opportunities for cybercriminals are obvious.

Distributed work environment and unprotected mobile technology – Real estate agents and brokers are mobile-first and must move quickly during a purchase or sale. With an increasingly mobile workforce, employees are no longer confined to a work environment protected by perimeter security appliances. Today, roaming laptops and mobile devices need to be protected regardless of location, operating platform, or device ownership.

Adoption of cloud applications – The real estate industry is quickly moving into the cloud age, and is heavily reliant on internet-based operational processes and information sharing. This means more systems that could potentially be targeted and affected by attacks.

Large amounts of stored personal & financial information – Real estate brokers and agents possess significant amounts of confidential third-party information stored on their computing devices or in their email, in the form of names, addresses, emails, credit reports, social security numbers, or contracts and financing terms.

Phishing and hacking scams stealing money and dreams

In the last few years, targeted phishing attacks like business email compromise and impostor emails, as well as malware attacks of many types, have become prominent in the real estate industry.

- **Reported Attacks Up 480%:** In 2017, the FBI warned of the dramatic increase in cyberattacks specifically targeting real estate companies. The number of inbound complaints to the FBI reporting such cyberattacks grew 480% between 2016 and 2017.
- **Escrow Fraud:** In 2017, cyber-criminals stole client contact information from a DC-area real estate company, which resulted in $1.5 million being stolen in a phishing wire fraud scheme from a couple about to close on a home.
- **Data Theft:** In 2015, a Manhattan-based real estate company's commercial property database for 7,000 neighborhoods was stolen by a hacker.

> "With sophisticated hacking mechanisms, a perpetrator will target weakly guarded transactions and, for instance, send the buyer an email from an address nearly identical to the closing agent's, with a plausible subject line, advising of a "wiring change"."

STATE ADVISORY ON REAL ESTATE WIRE TRANSFER FRAUD, APRIL 10, 2018

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

10 Steps to Protect Your Real Estate Business

Solution Brief

The Business Impacts of a Breach

Among the potential risks that real estate businesses need to protect against are:

Financial fraud – Business email compromise attacks and impostor emails divert funds to criminally-controlled accounts, with both the customer and the real estate firm potential targets for the stealing of funds. Lost revenue can also result from reputation damage and lost customers.

Data theft – Phishing attacks use spoofed email messages and copycat websites that look legitimate to trick victims into sharing valuable personal or business information, such as market research data, customer contact data (names, addresses, emails), financial account information (bank account numbers, transaction data), social security numbers, and credit data (including possibly credit card information).

Reputation and loss of business – Real estate companies risk major reputation damage and loss of clients and future business if their company is phished and money or data stolen.

Business interruption – Real estate businesses are driven by fixed closing and settlement dates, sales cycles, and scheduled meetings to ensure profitability and customer satisfaction. It only takes one phishing or malware attack to have a detrimental effect on an entire sales cycle, leading to financial consequences.

What you can do to protect your company, business partners, and customers

1. **Deploy endpoint security with active/behavioral monitoring.** Malware and ransomware evolve quickly and you need to augment traditional AV with next-generation detection.
2. **Deploy a web security gateway.** An effective web security gateway will stop new and zero-day malware downloads, attempts to access malicious URLs, and communications with botnet C&C servers.
3. **Deploy cloud-based email gateway protection from a security provider.** Cloud-based secure email gateways add more advanced security like time-of-click URL analysis and protection from business email compromise.
4. **Develop a formal wire transfer policy.** Institute a company-wide policy that prevents any financial disbursements based solely on emailed requests, including creating methods and procedures for buyers and sellers to authenticate any payment instructions received by email.
5. **Protect mobile users while they are working outside the office.** Laptops and smart phones are fundamental business tools as email and texting activities are critical for agents to get their jobs done. Get protection that follows your users.
6. **Use a password management tool and multi-factor authentication.** Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords will likely be exploited to access other systems.
7. **Protect against evasive threats with sandboxing.** Today's malware developers are incorporating many different tactics to evade detection by traditional technologies. A cloud sandbox array is a new capability that can sit in-line with an email security gateway to protect from today's evasive malware.
8. **Patch early, patch often.** Outdated operating systems, browsers, and plugins are major vectors for malware infections.
9. **Turn off network shares and unnecessary admin rights.** Current malware exploits sharing vulnerabilities and seeks out mapped network drives.
10. **Train users.** Educate users about the social engineering tricks that are used.

Consult us about Cyren's security services:

Email Security Cloud Sandboxing DNS Security

www.Cyren.com

sales@cyren.com