CASE STUDY

THE KEYES COMPANY

REAL ESTATE

UNITED STATES

CYREN EMAIL SECURITY PLUS

CYREN

Real Estate Firm Confronts Office 365 Phishing

In operation since 1926, The Keyes Company is a leading real estate firm in the southeastern United States, providing services to customers in six Florida counties, as well as real estate sales expertise to clients in several foreign countries. With over 3,500+ associates working in over 50 offices, The Keyes Company prides itself on not only the deep first-hand knowledge it brings to each transaction, but its integrity and commitment to the well-being of its employees, agents, and customers.

> "Since installing Cyren Email Security, we've observed an 85% reduction in phishing emails getting through to users, and a 27% drop in tech support calls."
>
> **Wendi Iglesias, Chief Information Officer, The Keyes Company**

PROTECTING AGENTS, CUSTOMERS, AND NETWORK

While all Keyes employees possess an email account, the real estate agents, in particular, connect to corporate systems multiple times throughout the day, often from the road or different office locations. Smart phones are a necessity and secure mobile communications and connectivity are critical for the agents to get their jobs done.

In real estate-focused cyberattacks there are often two primary victims: the customer whose funds are stolen and the company whose infrastructure and operations are compromised. In addition, there are sometimes secondary victims—such as partners, vendors, and suppliers whose information is also stolen during the breach. As a member of Leading Real Estate Companies of the World (LeadingRE), a network of over 500 global real estate brokerages, The Keyes Company also recognized that other real estate firms in their network, as well as those firms' customers, could become victims if Keyes were breached.

Keyes felt strongly about protecting their customers first and foremost, as well as their associates, their partner network, and their brand. They knew they needed to take proactive steps quickly to strengthen their cybersecurity.

PHISHING INUNDATING USERS AND SUPPORT

By 2017, firm executives realized that the entire real estate industry had become one of the biggest targets for phishing—usually in the form of business email compromise (BEC) or imposter email attacks—in which an email appears to come from a known partner, vendor, or even a colleague within the company, with the ultimate goal of stealing money through wire transfer or escrow fraud.

The escalation in attacks was due to the industry's role in facilitating high volume, high dollar figure wire transfers, as well as the highly sensitive personal information held by real estate firms in the form of customer names, addresses, emails, social security numbers, and bank information.

CASE STUDY:
THE KEYES COMPANY

Email Security

The company began to experience its own significant uptick in phishing attacks, as its employees and associates were getting hammered on a daily basis by phishing emails. At peak, the IT support team was receiving 1,100 tickets per month, of which approximately 30% were phishing.

The company had assumed that their email service—Office 365—would provide the necessary protection from phishing. However, they quickly learned that additional measures would need to be taken to confront the increasingly stealthy and varied phishing threats appearing on a daily basis.

CHOOSING AN EMAIL SECURITY SERVICE

Operational activities with most real estate companies today take place in the cloud. The Keyes Company is no exception. This fast-paced, high-volume company required a security solution that operated at the same speed as both the cloud and new and emerging threats. A robust user training program had already been established, but the executives recognized that training alone was not enough—they needed automated, systematic protection.

With a cloud-based email infrastructure, the firm felt strongly about adopting a cloud-based email security solution, particularly given the distributed nature of the company's employees and associates. In addition, Keyes wanted a solution from a security provider that had proven experience in stopping phishing attacks. After evaluating a number of email security options, the company selected Cyren based on its ability to detect and stop phishing, its ease of deployment across the company's 50+ locations, and its competitive pricing.

85% LESS PHISHING REACHING USERS

Cyren's 100% SaaS email security gateway complemented Keyes' Office 365 infrastructure and delivered the deployment flexibility and low total cost of ownership (TCO) desired. Cyren's unique protection technology included impostor email detection, as well as real-time threat detection that is never out of date. Ultimately, Cyren delivered the fastest and most complete results over traditional appliance and hybrid solutions on the market.

Since installing Cyren security services, The Keyes Company has observed a dramatic 85% reduction in phishing emails, as well as a noticeable 27% decline in inbound tech support calls and tickets.

THE CHALLENGE

- A highly distributed real estate organization with over 50 office locations.
- A total "on the road" mobile workforce of 3,500+ agents that used their own smart phones to conduct business via email and texting.
- A strong desire to protect customers from fraud and financial loss.
- A desire to protect their real estate associates from fraud and nuisance, recognizing that training was not enough and that all it would take is one phishing email tricking one associate.
- Large numbers of phishing emails getting through to The Keyes Company's users. Office 365 was not stopping the attacks.
- Operating in an industry that is a noted target for cyberattacks. Real estate firms handle or participate in communications on a high volume of wire transfers and large sums of money, as well as personal information about buyers and sellers.

THE SOLUTION

- Cyren Email Security Plus

THE CYREN DIFFERENCE

- Phishing attacks reduced by 85%.
- Cyren provided a free formal Email Security Gap Analysis, an assessment which quantified the severity of the security problem with their current solution.
- Risk of infected mobile devices or laptops entering the network greatly reduced.
- Demands on IT staff time for remediation of suspicious emails reduced by 27%.
- All employees protected wherever they are, even without connecting via VPN to the corporate network.